Management of Operational Risks related to Information Security in Financial Organizations

Authors
Rajia Rafique (06-12-1987)
Furhan Mehmood (10-08-1982)

Supervisor    Dr. Deepak Gupta
Examiner      Dr. Michael Le Duc

Seminar Date: June 3rd, 2010

School of Sustainable Development of Society and Technology (HST)
Acknowledgements

All praises to Almighty Allah who bestowed me with everything and always helped me at every step of my life. I would like to express my sincere gratitude towards my supervisors, Dr. Michael Le Duc & Dr. Deepak Gupta for giving me an opportunity to work on this challenging topic and for providing continuous feedback during the course of this work.

I am grateful to my family without whom I could never be where I am today. I am deeply grateful to my father for always believing in me and supporting me with his love and patience, specially my mother who has always been a great source of inspiration and motivation all the way throughout my life. I would like to dedicate my work to “Noshaba Malik” for always standing beside me and never giving up on me.

Lastly, thanks to all my friends and colleagues who took active interest in this project specially Ms. Rabia Durrani, Mr. Mehmood Zia-ud-din and my group member Rajia Rafique.

Furhan Mehmood

June 2010
Acknowledgements

Above all, thanks to Almighty Allah who has given me strength and conferred on me special favors throughout my life.

I would like to express my gratitude to all those who have contributed to this research work specially my supervisors; Dr. Michael Le Duc and Dr. Deepak Gupta and my thesis partner Furhan Mehmood.

I would like to dedicate my work to my Ami and Abu for their love, devotion, and prayers throughout my life. I owe my loving thanks to my siblings for their trust and support. I would like to thank my family from the bottom of my heart.

Thank you all

Rajia Rafique

June 2010
Abstract

Date: 30th May 2010

Authors: Rajia Rafique, Furhan Mehmood

Tutor: Dr. Michael Le Duc, Dr. Deepak Gupta

Title: Management of Operational Risks related to Information Security in Financial Organizations

Introduction: Information security is very significant for organizations, especially for financial organizations where customer information and their satisfaction are considered the most important assets for financial organizations. Therefore customer information must be sustained from information security breaches in order to satisfy customers. Financial organizations use their customer’s information several times a day to deal with different operations. These operations contain several types of risks. Operational risks related to information security are becoming sensational for financial organizations. Financial organizations concentrate to reduce the exposure of operational risk related to information security because these risks can affect the business to a great extent. Financial organizations need such policies and techniques which can be used to reduce the exposure of operational risk and to enhance information security. Several authors discuss about several types of operational risk related to information security, and several authors discuss about the techniques to avoid these risks in order to enhance information security.

Problem: Investigate the concept of Operational Risks related to Information Security and how it is perceived in Financial Organization?

Purpose: The aspiration of writing this report is to describe and analyze operational risks related to information security in financial organizations and then to present some suggestions in form of polices or techniques which can be used by financial organizations to enhance their information security.

Method: Since the type of our thesis is Qualitative based, therefore exploratory research approach is used to carry out research. Authors tried to use secondary source of information as well as primary source of information in order to get maximum knowledge about the topic and to come up with maximum possible output.
Target Audience

The target audience in our mind for this paper consists of both, academic readers and professionals who have interest and some knowledge about information security and operational risks. Target audience for this research work includes professionals, academic readers and both investigated organizations (NCCPL and CDC).

Conclusion

By critically analyzing the literature written by various authors and the worthy information provided by our primary sources gave us the opportunity to develop a solution to keep the operations secure from risks and to fix the current problems related to information security. We found that there are different types of operational risks related to information security which can affect the business of financial organizations and there are various techniques which can be used by financial organizations to solve the current issue related to operational risks in order to enhance information security. It was also found that top management in financial organizations is interested in issues about information security operational risk and they showed their keen interest in adopting new effective techniques.

Keywords: Information Security, Information Security Risks, Operational Risks, Operational Risk Management, Operational Risks in Financial Organizations.
## Contents

1.0 **Introduction** ........................................................................................................................................ 1  
1.1 General /Background ......................................................................................................................... 1  
1.2 Problem Statement ............................................................................................................................ 2  
1.3 Research Question(s) ...................................................................................................................... 3  
1.4 Objective and Purpose of the Research ........................................................................................... 3  
1.5 Target Audience .............................................................................................................................. 3  

2.0 **Theoretical Framework** .................................................................................................................. 4  
2.1 Review of appropriate literature ...................................................................................................... 4  
2.2 Information Security Overview ........................................................................................................ 4  
2.3 Information Security Model .............................................................................................................. 4  
2.3.1 Availability ..................................................................................................................................... 5  
2.3.2 Integrity ......................................................................................................................................... 5  
2.3.3 Confidentiality ............................................................................................................................. 5  
2.3.4 Authentication ............................................................................................................................ 6  
2.4 Information Security Management System ...................................................................................... 6  
2.5 ISO Standards of Information Security Management System (ISMS) .............................................. 7  
2.6 Information Security Management Policies ...................................................................................... 8  
2.6.1 Access Control ............................................................................................................................ 8  
2.6.2 Email Usage Policy ...................................................................................................................... 9  
2.6.3 Internet Usage Policy .................................................................................................................. 9  
2.6.4 Password Management Policy ................................................................................................... 9  
2.6.5 System Usage Policy .................................................................................................................. 10  
2.6.6 Incident Handling Policy ............................................................................................................ 10  
2.7 Risk .................................................................................................................................................. 10  
2.8 Operational Risks and its Types ....................................................................................................... 11  
2.9 Operational Risks in Financial Organizations .............................................................................. 12  
2.10 Operational Risk Management ..................................................................................................... 13  
2.11 General Risk Management Approach .......................................................................................... 14  
2.11.1 Risk Avoidance ......................................................................................................................... 15
2.11.2 Risk Reduction.................................................................................................................. 15
2.11.3 Risk Transfer..................................................................................................................... 16
2.11.4 Risk Retention.................................................................................................................... 16
2.12 Impact of Operational Risks on Business............................................................................. 16
  2.12.1 Reputation Loss.............................................................................................................. 17
  2.12.2 Financial Loss ................................................................................................................ 17
  2.12.3 Business Demolish ....................................................................................................... 17
2.13 Management Commitment and Involvement....................................................................... 17
2.14 Conceptual Framework ......................................................................................................... 18

3.0 Research Design/Methodology ............................................................................................. 21
  3.1 Choice of Topic .................................................................................................................... 21
  3.2 Research Approach ............................................................................................................ 21
  3.3 Research Process ................................................................................................................ 21
  3.4 Data collection and source ............................................................................................... 22
  3.5 Method critique .................................................................................................................. 23
  3.6 Sampling Strategy .............................................................................................................. 23
  3.7 Design of Questionnaire ................................................................................................. 24
  3.8 Data Analysis ...................................................................................................................... 25
  3.9 Framework of Methodology ............................................................................................. 26

4.0 Empirical Study .................................................................................................................. 27
  4.1 Interview Guide .................................................................................................................. 27
  4.2 Findings ............................................................................................................................. 27
    4.2.1 NCCPL ......................................................................................................................... 27
      4.2.1.1 Operational Risk .................................................................................................. 27
      4.2.1.2 Information Risk Management ........................................................................... 27
      4.2.1.3 Structure of Organization .................................................................................. 28
      4.2.1.4 Operational Risk and Threats .......................................................................... 28
      4.2.1.5 Management Commitment and Involvement .................................................... 30
      4.2.1.6 Impact of operational risks on business .............................................................. 31
    4.2.2 CDC ............................................................................................................................ 31
List of Figures

Figure 1: Information Security Factors ................................................................. 6
Figure 2: Figurative description of Information security management system (ISMS) ........................................ 7
Figure 3: Operational Risk ..................................................................................... 12
Figure 4: Risk Management cycle ......................................................................... 14
Figure 5: Operational Risks impact on business ...................................................... 17
Figure 6: Conceptual Model ................................................................................... 20
Figure 7: Component for data analysis: interactive model .................................... 25
Figure 8: Framework of methodology .................................................................... 26

List of Tables

Table 1: Operational Risk Model ............................................................................ 13
Table 2: Operational risks, solutions and impacts on business ............................ 41
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRO</td>
<td>Chief Risk Officer</td>
</tr>
<tr>
<td>CEO</td>
<td>Chief Executive Officer</td>
</tr>
<tr>
<td>COO</td>
<td>Chief Operating Officer</td>
</tr>
<tr>
<td>CTO</td>
<td>Chief Technical Officer</td>
</tr>
<tr>
<td>CDC</td>
<td>Central Depository Company of Pakistan</td>
</tr>
<tr>
<td>ISMS</td>
<td>Information Security Management System</td>
</tr>
<tr>
<td>IEC</td>
<td>International Electro technical Commission</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>NCCPL</td>
<td>National Clearing Company of Pakistan Ltd</td>
</tr>
<tr>
<td>TL-RBAC</td>
<td>Three Layer Role Based Access Control Framework</td>
</tr>
</tbody>
</table>
1.0 Introduction

This chapter begins with background and introduction of our dissertation. It further presents the problem statement, research questions, objective and purpose of the research, limitation and target audience in order to explain the structure and purpose of the study.

1.1 General/Background

Information security is a core issue in most organizations because development in distributed processing has made it easier to access information. As a consequence organizations want to assure the protection of their information (Solms et al., 1998). Information security is needed because the technology applied to information creates risks (Blakley et al., 2001). Organizations try to protect their information by protecting their information technology environment (Solms, 1999).

In the beginning of computing, mainframe computers were used with single processors, there was no shared database, and only one program was executed at a time. It was easy to secure such an environment. A few technical and physical mechanisms were enough to secure the entire information processing environment. Later the computing revolution and multi-processing computing creates a number of additional technical security mechanisms. More technical and procedural mechanisms were required to secure such an environment (Solms, 1999).

Despite the fact that financial organizations have faced up operational risks all the way through their history, the special attention and focus towards the management of operational risks has increased to a great extent in the past several years. This special attention and focus on operational risk is because of two main developments which are: an increased emphasis on the transparency in the financial reporting of an organization, and increased exposure to operational risk forced by new and complex production of technologies used by financial organizations. Though new technologies bring down the costs of production and increase the value of the product, but it also creates operational risks (Cummins et al., 2006).
Development in technology has given the opportunity to financial organizations to provide products and services online. The fast development in technology provides benefits but at the same time it contains operational risks too (Fontnouvelle et al., 2003).

The main focus of this study is to address information security operational risks and their impacts on business in financial organizations. Information in financial organizations is very sensitive as most of financial services are allowing customers to perform online financial transactions through the internet and even on mobile phones; which introduces new questions in terms of information security and risks.

1.2 Problem Statement

Information Security is important according to the dependency of organizations on information technology (Blakley et al., 2001). Nowadays organizations are more technology dependent than ever before and therefore security risks have increased. Many organizations provide online services which involve new risks; outsourcing adds more information security risks (Lachello, n.d.).

Nowadays many financial organizations link their computer networks to the internet to provide services to their clients or to connect with the computer networks of their business partners. Therefore information can be lost to a great extent. Information security policy cannot regulate the users outside an organization because it only regulates the behavior of users in an organization. Under these circumstances, it is required to have a secure IT community to ensure a secure IT environment (Solms et al., 1998).

Technical security controls need support from appropriate operational controls in order to implement a secure IT environment. These operational controls will be used to handle the actions and behavior of users when they are dealing with information (Solms, 1999).

Information security plays a vital role in a financial organization. A financial organization needs to pay special attention to manage its information security in order to keep continuous flow of its daily operations consistent and reliable.
1.3 **Research Question(s)**

*Investigate the concept of Operational Risks related to Information Security and how it is perceived in Financial Organizations?*

a. What are the operational risks related to Information Security in financial organizations?
b. How these operational risks can affect the business in financial organizations?
c. How much top management is aware, involved and committed in information risk management?
d. How these problems/issues can be solved to enhance the information security?

1.4 **Objective and Purpose of the Research**

It seems that many people know about the risks involved in information security, but actually a few of them have real idea about these risks. It is because information security can be considered from different aspects such as different aspects of business processes, technology, organizations and individual behavior (Kajava et al., 2006).

In this study, we intended to describe and analyze the operational risks related to information security with respect to financial organizations. After significant investigation identified operational risks were analyzed in order to provide a solution to enhance information security.

1.5 **Target Audience**

The target audience in our mind for this paper consists of both, academic readers and professionals who have interest and some knowledge about information security and operational risks. The reader will be able to know in depth details regarding operational risks and threats related to information security within financial organization. Furthermore our targeted organizations which include CDC and NCCPL are also included in target audience. CDC and NCCPL can go through our research work in order to enhance information security in their organizations.
2.0 Theoretical Framework

The purpose of this chapter is to provide the conceptual framework and literature review. The literature review consists of critically analyzing relevant literature written and conceptual framework presents the impacts of information security operational risks on a financial organization.

2.1 Review of appropriate literature

The literature related to our research is categorized as:

- Information security
- Operational risks
- Impact of operational risks on business
- Management commitment and involvement

2.2 Information Security Overview

The objective of information security is to secure the information systems and data in them, in order to ensure integrity, availability and confidentiality (Kajava et al., 2006).

Information security is the term that describes the need to protect information that based upon the fact that information is classed as a valuable asset (Mitrovic, 2005).

Information security is no more an internal matter of an organization. In this era of electronic commerce, information security of an organization affects its partners. Therefore organizations demand their business partners to demonstrate some information security mechanisms in order to satisfy that information is secured. An organization can use information security standards in order to demonstrate that security mechanisms are being used to protect information (Solms, 1999).

2.3 Information Security Model

Information security breaches are categorized as incorrect data modification, unauthorized data observation, and data unavailability. Unauthorized data observation can cause the disclosure of information to the users who are not allowed to get access into the system. Incorrect data modification leads to an incorrect state of database and incorrect data can lead all organizations like healthcare or a financial organization to bear heavy losses from financial perspective as well
as human perspective. When information is not available, it can cause the business of a financial organization in terms of financial losses as well as reputation losses. According to Sandhu and Bertino (2005), information security model can be used in organizations in order to secure the information from information security breaches. The information security model defined by Bottino and Hughes (2006) is composed of availability, integrity, confidentiality and authentication.

2.3.1 Availability

Availability is a broad term as it comprises many aspects. It is defined as a computer resource which makes the information objects available (Hedenstad, 2009). Or according to Bottino and Hughes (2006) “It is the state of being ready to use. The attribute of availability is specified as being approachable and it prevents the denial of service issues”. In information security, availability means to have information available for the valid users and if the information is not present then confidentiality and integrity have no use (Furssell, n.d.).

2.3.2 Integrity

The property of integrity defines that data is present without any modification from unauthorized users. Integrity of data means that data has not been lost or changed and maintains the data in its original form (Bottino & Hughes, 2006).

Some constraints and mechanisms are applied together to ensure the integrity of data. When an unauthorized user attempts to change the data, at that time access control mechanism checks the rights for that user whether he has sufficient rights to access and change the data, and then semantic integrity subsystem checks the correctness of data (Sandhu & Bertino, 2005).

2.3.3 Confidentiality

Confidentiality ensures that data is only available to authorized users (Bottino & Hughes, 2006) by using access control mechanism. When a user attempts to get access of data, the mechanism verifies the rights for that individual. Confidentiality can be accomplished by hiding or preventing the data from unauthorized access (Sandhu & Bertino, 2005).
2.3.4 Authentication

Authentication is another parameter of information security which is used to authenticate the identity of the user (Bottino & Hughes, 2006). It will allow the valid user to get access into the system.

![Information Security Factors](image)

**Figure 1: Information Security Factors, Source: Authors**

2.4 Information Security Management System

Information security management system performs a significant role in an organization’s security implementation (Norman & Yasin, 2009) by considering all aspects in an organization that handles with creating and maintaining a secure information environment (Eloff & Eloff, 2003). The successful implementation of ISMS needs particular involvement and contribution from all employees, starting from senior management to end users. ISO security related standards lead organizations about certain requirements and demands (Dey, 2007).

The purpose of Information Security Management System is to provide right information on right time to a right person at a right place.
In order to achieve the main purpose of ISMS, it is divided into two levels; System level ISMS and Process level ISMS. According to Bundesamt fur Sicherheit in der Information-stechnik (BSI), (2004) “the process-level contains several sub processes such as development, planning, implementation, evaluation, and maintenance of IT security. The System-level in contrast is concerned with the orchestration of the Process-level’s tasks. It contains matters like organizational structure, responsibilities, processes and resources.” (Huber et al., n.d.).

2.5 ISO Standards of Information Security Management System (ISMS)

The process ISMS encourages the implementation of the controls which contained in a standard, for instance ISO17799. A Standard includes technical specifications which concern to the aspects like Information Technology network and access control etc. (Eloff & Eloff, 2003).

There are many different standards that can be used in ISMS, for instance ISO 9001, ISO 17799, BS 16000, ISO Guide 62, TR13335, Common Criteria etc (Eloff & Eloff, 2003).

The international standards provide effective practices related to information security; for instance practices of effective management of information security, managing the problems related to portable devices, internet and wireless technology. ISO/IEC 17799 is the standard for information security management. It offers a common language for information security that
makes it feasible for organizations to communicate with other organizations on same level. After ISO/IEC 17799 standard, the international standardization committee developed another standard for information security management named as ISO/IEC 27001 standard (Kajava et al., 2006). In the respect of ISO standards, the series related to 2700x is considered as a dedication to information security management system (Varafort et al., n.d.).

ISO 27001 is one of the most important standards in the series of ISO 2700x (Michael Huber, et al., n.d., pp. 146), which is transposed from a standard called BS 7799-2:2002(Varafort et al., n.d.). ISO 27001 defines the key requirements for planning, establishing and implementing information security management systems (Huber et al., n.d.).

ISO/IEC 27001 was developed to protect the information assets of all type of businesses. The information security management system standard was developed to secure the information cost effectively and risk management is the main focus of this standard (Humphreys, 2006).

### 2.6 Information Security Management Policies

There are several policies which can be used to tighten up and strengthen the information security management system.

#### 2.6.1 Access Control

There are various techniques which can be used to enhance information security. Access control is the one of these techniques which is extensively used to maintain the information and information systems secure and consistent (Zhongping et al., 2008). Access control is substantial to protect data from unauthorized modifications (Hagen et al., 2007).

An organizational structure frequently deals with the change of employees which results to change of access rights and information. To change the access rights so frequently creates difficulties for administration (Zhongping et al., 2008).

An organization needs an access control system which can specify who can get access to particular information. To control these problems right access control measures are required (Hagen et al., 2007).
Access Control is a policy which assures that the request from authorized user is accepted and request from unauthorized users is rejected (Wen & Wu, n.d.).

Organizations may be exposed to various types of threats because of the weaknesses in access control. (Hagen et al., 2007).

There is huge amount of sensitive and confidential information in a financial organization, for instance credit card number etc. That is why in financial organizations high levels of information security are required. An appropriate access control framework is required in order to achieve high levels of information security. The commonly used access control framework has some drawbacks in it and it does not fulfill the requirements of a financial organization although it offers an effective access control model that can bound the operations of different users. So for financial organizations, a Three Layer Role Based Access Control Framework (TL-RBAC) is suitable. TL-RBAC fulfills the requirements of a financial organization by implementing access control in three levels; web pages, operations, and data (Wen & Wu, n.d.).

2.6.2 Email Usage Policy

An organization supports and encourages the responsible use of email services but accepts that email is not a confidential means of communication. Email services can be used inappropriately and cannot always protect users from receiving email contents that an organization may consider offensive. However all reasonable efforts are applied in order to mitigate the abuses of the Email service (Saran & Zavarsky, 2009).

2.6.3 Internet Usage Policy

The purpose of Internet Usage Policy is to establish rules to ensure that usage of the internet complies with the company’s Information Security Policy, to protect the company against damaging legal consequences, and to educate the individuals who may use the internet with their responsibilities associated with such use (Saran & Zavarsky, 2009).

2.6.4 Password Management Policy

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the company’s entire
corporate network. The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change (Wood, 1997).

2.6.5 System Usage Policy

The purpose of system usage policy is to describe the appropriate use of computer equipment in an organization. Inappropriate use exposes the organization to various risks including compromise of services, compromise of networks, virus attacks, information leakage and legal issues. Every computer user is responsible to know these guidelines, and to conduct their activities accordingly (Feng et al., 2007).

2.6.6 Incident Handling Policy

*Incident Handling Policy* outlines the requirements, communicates how an incident shall be handled and provides basis for enforcement of incident handling procedures and practices. The main function of this policy is to ensure that the incident is reported and handled in a structured and timely manner (Geneiatakis et al., 2009)

2.7 Risk

According to Marshall (2001), risk can be broadly defined as the “potential for events to cause future losses or fluctuations in future income”.

**Characteristics of Risks**

Taylor (2004) describes the characteristics of risk into three categories:

1- The event (i.e. any positive or negative event occur in the system)

2- Event occurrence probability (i.e. what is the possibility of happening that event)

3- Impact on projects (when at last the event occurs what would be its consequences, negative or positive)

A risk analysis shall identify everything that could go wrong in an organization, what is the probability of its occurring and what consequences it might create. Author further states that: “Within the core of best practices is the security risk assessment” and this is a valid statement
that if one understands that without the knowledge of the risks no one can take action against them (Landoll, 2005).

### 2.8 Operational Risks and its Types

“Operational risk 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” (Philip, 2009).

According to Hussain (2000) there are various types of operational risks such as:

- Business Continuity Risk
- Personal Risk
- Organizational Risk
- Strategic Risk
- Reputation Risk
- Currency Risk
- Change Management Risk
- Regularity Risk
- Portfolio Risk
- Legal Risk

According to Marshall (2001), operational risks can be defined as “residual risks, i.e. everything that is not credit or market risk”.

Saunders (2000) advocates about operational risk that internal sources of operational risks are technology, capital assets destruction, customer relationships and employees. External sources are natural disaster and fraud etc.

Operational risks are further divided into two areas, operational leverage risk and operational failure risk. An operational failure risk is the failure of information systems, processes and people. The risk factors in these types of risks are primarily internal. On the other hand operational leverage risk is the risk when the firm’s operations will not generate the profit as expected because of external factors involved such as changes in political, legal environment or in the nature of the competition (O’Brien et al., 1999).

Bessis’ (1998) considers operational risk in another way, according to his views operational risk is divided into two levels; first level is technical level that consists of issues such as when information system or risk measure have some deficiency, the second level consists of more
organizational characteristics having monitoring and reporting of risk and all related rules, regulations and procedures. Bessis’ (1998) definition also implies that a lot of operational risks evolve from information technology.

![Figure 3: Operational Risk, Source: (Finance Wise, 1999)](image)

### 2.9 Operational Risks in Financial Organizations

Within financial organizations operational risk can be defined as “the entire process of polices, procedure, expertise and systems that an institution needs in order to manage all the risks resulting from its financial transactions” (Hussain, 2000).

According to Elke (2003, pp. 927), operational risks related to information security in financial organizations have been divided into two main categories:

- Internal Risks
- External Risks

**Internal Risks**

Internal risks are those risks which affect the organization from inside and further sub-divided into three categories.

- System Risks
- Process Risks
- Personal Risks
External Risks

External risks are those risks which affect the organization from outside.

<table>
<thead>
<tr>
<th>Risks main relevance</th>
<th>System Risks</th>
<th>Process Risks</th>
<th>Personal Risks</th>
<th>External Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational Risks</td>
<td>Damage through programming bugs, viruses, infections</td>
<td>Inappropriate operational procedures</td>
<td>Dependency on external personnel for maintenance</td>
<td>Network damages, power breakdown</td>
</tr>
<tr>
<td></td>
<td>Backup failure, loss of data</td>
<td>Unauthorized use(beyond defined responsibilities)</td>
<td>Insufficient organizational personnel embedding</td>
<td>Unauthorized access, destructive hacks</td>
</tr>
<tr>
<td></td>
<td>Shortcomings/defect of human –machine-interfaces</td>
<td>Workflow interdependencies during transactions processing</td>
<td>User error (intentionally or unintentionally)</td>
<td>Fraud/vendors</td>
</tr>
</tbody>
</table>

Table 1: Operational Risk Model, Source: Authors, based on: (Elke Wolf, 2003, pp.927)

2.10 Operational Risk Management

Risk management is about identifying risk, risk avoidance (before occurrence), risk defense (during occurrence), recovery (after occurrence) and improvement (enhance risk management plan). Risk management is not a onetime process; it is an ongoing activity (Olzak, 2007).

Human judgment plays an important role in the decision making process. Decisions regarding risk and uncertainty cannot always be made in a complete objective manner, political and physiological issues are also present (Edward & David, 2007)
Rebecca Herold (2005) states: “Prevention is much less expensive than response and recovery” in the book “Managing and information security, privacy awareness, training program”. This statement summarizes the thoughts behind risk analysis and information security.

### 2.11 General Risk Management Approach

As discussed earlier, almost all organizations face risks, whether they are financial risks, information risks or operational risks. A generalized procedure to manage risks, consists of five stages as shown in below figure; risk identification, risk estimation, risk evaluation, risk response and risk monitoring (Baker et al., 1998).

**Figure 4: Risk Management cycle, source: (Baker et al, 1998)**

Risk analysis phase consists of risk identification stage and risk estimation stage, this phase identifies threats that comprise risks to the organizations. Next phase is risk evaluation phase, which evaluates to what extent the risk might affect the business. The last phase is called risk control phase and it consists of risk response stage and risk monitoring stage. Now it depends on the organization’s need to decide how to manage these risks and then monitor the preventing actions (Baker et al., 1998).
It is not affordable for companies to address every threat to the availability and security of IT infrastructure with same hostility. Even if they want to do that it would not make any business sense. So risks must be categorized and addressed according to their probability to occur and their priorities. Management actions to alleviate risks must be prioritized with an eye to their cost and impending benefits (Applegate et al., 2007).

In spite of the fact that how complex the risks within the organization, there are four possible approaches to manage risks which are: risk avoidance, risk reduction, risk transfer and risk retention. Risk avoidance and risk reduction are referred as risk control because they minimize the organization’s overall exposure to risk. On the other hand risk transfer and risk retention are considered as risk financing and the goal is to ensure that the funds are available to recover the losses (Shimpi, 1999).

We will briefly describe each approach below:

2.11.1 Risk Avoidance

“A firm can elect to abstain from investments with payoffs that are too uncertain” (Shimpi, 1999). All of the activities that create risk can be avoided or by substituting less risky processes (Doherty, 2000). Each organization has different requirements, on the basis of these requirements they will draw lines between acceptable and unacceptable risks. The decision concerning where to draw the lines depends on the internal and external factors, so risk avoidance reflects each organization’s needs to maintain its focal point and choose its battle (Shimpi, 1999).

2.11.2 Risk Reduction

An Organization can limit its downside risk of processes by monitoring its progress, through continuous inspections and regular evaluation of its efficiency, which is also a loss control technique (Shimpi, 1999).

“Risk reduction occurs through loss control, diversification and loss prevention. Loss prevention seeks to reduce the likelihood of a given type of loss occurring and examples of loss prevention measure include safety devices like burglar alarms and smoke detectors” (Doherty, 2000).
2.11.3 Risk Transfer

Risk can also be transferred from one party to another party that is better equipped or more willing to bear it (Shimpi, 1999). For example, the risk can also be transferred to another party by purchasing insurance policy or outsource your critical part (Doherty, 2000).

2.11.4 Risk Retention

In some cases organizations also retain a variety of risks, voluntarily or involuntarily. Voluntarily risk retention means a conscious decision to absorb the risks, because it is the most effective way to addressing the risk. (Shimpi, 1999) Involuntarily risk retention occurs when the business fails to recognize the exposure of upcoming risk (Doherty, 2000).

2.12 Impact of Operational Risks on Business

Operational risk from a business perspective can be viewed as a risk which comes through the production of goods and the services given to the clients of a financial organization (Cummins et al., 2006).

There are various risks in financial organizations but operations risks are considered the most important of them because they can destroy a business, either as a result of loss of reputation or loss of operation capability of company (Philip, 2009).

Chapelle et al (2004) states that “at the present time, the assessment of operational risk still remains a delicate endeavor, due in part to the intrinsic difficulty of the exercise, to its exploratory stage of development, to the scarcity of data, and to the new regulatory definitions of operational risk events and business lines of activity.”

Operational risk is associated to many factors, some of which are: complexity and type of different activities, information flows, and quality of management, processes, and the system. Therefore different financial organizations might experience different types of operational risks (Chapelle et al., 2004).

Operational risks include various events such as external fraud, internal fraud, clients, business practices, products, business disruption and system failures and execution, delivery and process management (Cummins et al., 2006).
2.12.1 Reputation Loss

Reputation loss with respect to financial organizations is defined as a loss which occurs as a result of damaged reputation about the financial stability of financial organization and causes the financial organization to have decreased number of customers (Vozrozhdenie Bank, 2009).

2.12.2 Financial Loss

Financial Loss can be defined as: “Loss of financial resources, assets or potential income” (Kovarik, 2006).

2.12.3 Business Demolish

Business demolish is a risk which can crush the business and consequently will destroy the business completely.

Figure 5: Operational Risks impact on business, Source: Authors

2.13 Management Commitment and Involvement

It is required for a financial organization to establish an effective risk management strategy. Many employees attempt to increase the profitability of their organization, but a few of them pay
their attention to risk management. It is therefore interesting to know about who are the concerned persons for establishing the strategy of risk management (Shimpi, 1999).

According to Shimpi (1999), the chief executive officer (CEO) is the person who is considered to be responsible for the success of an organization and therefore chief executive officer (CEO) is considered as risk officer. The CEO determines that how much the organization will bear the risk.

Correct information is the integral part of the organization because on the basis of this information, management is able to take any decision, wrong or ambitious information leads the management towards wrong decision (Edward & David, 2007).

According to Hussain (2000), top management plays a significant role when we talk about information risk management. Top management should ensure that culture, systems, organization’s structure and people are contributing to effective information risk management. Altogether, involvement of top management is essential for the success of an effective information risk management system (Kotulic & Clark, 2004).

In recent years, various organizations have appointed executives to positions like “vice president of risk management” or chief risk officer. The role of chief risk officer (CRO) is to develop effective strategies and to implement those strategies in order to decrease harmful effects of business losses on the organization (Shimpi, 1999; Kotulic & Clark, 2004; IAAC, 2003).

### 2.14 Conceptual Framework

The conceptual framework intended clearly in the (figure 6) elaborates the impact of information security operational risks in financial organizations. There are different types of financial organizations e.g. insurance companies, personal funds, credit unions, trust companies, investment funds, audit firms, banks and brokerage companies. The domain of our study is to investigate banks and brokerage companies.

Financial organizations have to deal with enormous number of internal and external operations every day. Internal and external operations contain internal and external risks which can affect the smooth running of the business of an organization. These internal and external operational risks can be like unauthorized use, backup failure, inappropriate operational procedures,
insufficient organizational personnel embedding and loss of data, unauthorized access, destructive hacks etc.

It has great significance for a financial organization to make smooth running of its operations because these operations are like the forces, which character the organization towards success and failure. The core purpose of this report is to analyze and evaluate the operational risks related to information security, its assessment and management from different perspectives and its affect on the business of a financial organization, which could drive an organization to achieve its goals and objectives in the long and short term.

There are three perspectives of information security i.e. administrative, technical and physical. Our focus is to cover the information security with technical perspective. Technical information security comprises of four characteristics which are availability, integrity, confidentiality and authentication.

The mentioned factors are mutually dependent on each other with some intervening factors. Concepts from Applegate et al, articles, journals, online materials and from primary data will be used for our research.
Figure 6: Conceptual Model, Based on: Elke Wolf, 2003, pp.929
3.0 Research Design/Methodology

The focus of this chapter is to explain the methods which are used to conduct and analyze the research. This chapter gives the information about method critique, sampling strategy, choice of topic, research process, data collection and source, sampling strategy, data analysis and framework of methodology.

3.1 Choice of Topic

Fisher (2007, pp. 31-33) states that the topic chosen for research should be interesting, relevant to your course and even excites you otherwise your motivation level will reduce after a certain time and that will create problems to complete the project. Furthermore the chosen topic should be approachable and there should be adequate literature available to write a literature and make a detailed analysis. In this regard our topic is quite interesting, relevant to our program and demanding in the market for IT Management students, researchers and business executives.

3.2 Research Approach

For the purpose of this research work, realist approach to research (Fisher, 2007) has been undertaken that considers both reality and knowledge.

As the qualitative nature of this research work demanded, to handle data concerning various subjective variables and then analyzing them objectively, realist approach to research seemed a best choice.

3.3 Research Process

Fisher (2007, pp. 153-155) discusses two approaches in his book “Researching and writing a dissertation” for discovering new things e.g. Explorers (Qualitative) and Surveyors (Quantitative). Qualitative research method will be used in this study because our research is of qualitative nature. The research has carried out by reviewing the available literature about operational risk related to information security and factors to improve the information security in financial organizations. Authors tried to get deep knowledge and understanding of the selected topic.
3.4 Data collection and source

The sources of information used in this research study comprises of both primary and secondary data. Biggam (2008) says that it is not only research strategy that determines quantitative or qualitative nature of research but it is combination of research strategy, research objectives and data collection techniques.

- **Primary Data**

  Shukla (2008, pp. 32) defines primary data as one that is “originated by researcher for the specific purpose of addressing the problem at hand”. Interviews were conducted in order to get primary data. The interviews were not structured to a great extent because our main goal was to carry out the questions with the interviewees, which could result in more discussions regarding the subject. Therefore we conducted a semi structured interviews. The aim of the interview was to get valuable information related to the topic of the thesis and research questions.

  There are different ways to conduct an interview. We used informant and respondent interview techniques to do so. Respondent interviews are used to conduct interviews with individuals who are engaged and present in the investigated area. On the other hand informant interviews are used to get information from the individuals who are not involved in the investigated area but have adequate information to provide about the topic (campbell, 1995).

  Primary data was collected from NCCPL (a financial company) and CDC (Financial company and custodian of stock shares). The type of interview conducted from the representative of NCCPL was a respondent interview and from CDC was an informant interview.

  There are three different types of interviews such as focus group interview, telephone interview, or a one-on-one interview. A telephone interview provides the best source of information when the researcher does not have direct access to individuals (Creswell, 2007). We conducted telephonic interviews through Skype with NCCPL and CDC, and then authors saved conversations with interviewees as audio files.
According to the problem definition and findings from the literature review, we came up with some interview questions. The well structured list of interview guide variables and questions can be found in Appendix 1.

- **Secondary Data**

Our second source of information was secondary data. According to Shukla (2008, pp. 30) secondary data is defined as “collection of data that already exists”. In order to develop conceptual framework and methodology chapters, authors have utilized various sources of information such as; articles, books, journals, online databases and MDH library like Elin@Malardalen, Emerald, IEEE Xplore and Compendex etc. The keywords used in finding appropriate literature were information security, information security risks, operational risks, operational risk management, operational risks in financial organizations etc.

### 3.5 Method critique

Because of the limited time frame, it was not possible for us to collect primary data from multiple companies and to include case studies in our research. The research is relied on primary data gathered from two companies. Access to certain articles which performed significant contribution to our research questions was limited in number because some payment was required to get access to those articles.

### 3.6 Sampling Strategy

Sampling strategy is a crucial part of any research. Sampling is “the process or technique of selecting a suitable sample from the whole population” in order to determine and generalize characteristics or parameters (Adams et al., 2007). Generally, cost and time are two important factors in the sampling process.

For the purpose of this master’s thesis, we have carried out two stages of sampling with various types of non-probability sampling method. According to (Bryman & Bell, 2007), non-probability sampling is an “umbrella term for a wide range of the types of sampling strategy based on common sense and best personal judgment”, outside the probability sampling. In the first phase,
authors have to decide the two companies as sample from the large-scale financial companies in Pakistan and secondly, management representatives or some concerned persons in the chosen companies were to select. In the first case, author’s utilized “purposive or purposeful” sampling (Fisher, 2007, pp. 191) because our both targeted companies are well established and national level financial companies in Pakistan. They provide fully automated electronics settlement services to their clients, so authors choose those companies for empirical data gathering. The second phase of sampling, however, is a mix of “purposive” and “convenience” sampling. According to (Bryman & Bell, 2007), not only that authors have had a purpose of “identifying the people who ... may be appropriate respondent for the questions” (Fisher, 2007, pp. 168 & 191) but also looked for the convenience of respondents’ accessibility, availability, and willingness to answer. Similarly, Greener (2008) defines that in convenience sampling, a sample is chosen for “ease or convenience rather than through random sampling”. Some other reasons, in support of authors’ choice of the mentioned sampling techniques, include the non-response issues; time and resource limitations; interview scheduling problems. By considering both factors purposeful and willingness to answer, authors have total of two respondents from two companies.

Hackley (2003, pp. 75) states that, generally, in qualitative research, sampling issues are resolved by necessity and are “often based on purposive or convenience criteria”.

3.7 Design of Questionnaire

As mentioned earlier, we followed telephonic interview technique to conduct interviews. Already prepared questionnaire is extremely helpful for interviewer to guide the flow of telephonic interview. Already prepared questionnaire provides help to keep the flow of interview on right track and it also ensures that interview does not miss any important question due to complexity of topic, number of variables involved, pressure of time, or simply because of human forgetfulness. Adams et al. (2007, pp. 145) says that for in-depth research interviews, a semi-structured approach should be used in developing a questionnaire which serves as ‘road map’ and guides throughout the interview. Nevertheless, such guides have essay type questions, developed as primary and secondary questions. The primary questions are more direct in nature and specifically related to the subject, whereas, secondary questions, also called sub-questions,
are used to probe deeper into the matter and may also depend on the possible response of the respondents. Open questions were asked in both interviews.

### 3.8 Data Analysis

Analysis of data is an ongoing and repetitive process, as a result of which latest components are introduced in a successful manner. Data comparison and data analysis will be performed by using qualitative approach. Analysis of primary and secondary data will give solution to the defined research questions (Miles & Huberman, 1994).

![Component for data analysis: interactive model](Miles & Huberman 1994 P. 12)

After finalizing the research topic, problem statement and research questions, appropriate literature was gathered from different sources. Afterwards primary information was collected from two financial organizations. We used Qualitative approach for comparing and analyzing primary and secondary information in order to come up with some conclusion/recommendation and the answers of our research questions.
3.9 Framework of Methodology

Figure 8: Framework of methodology, Source: Authors
4.0 Empirical Study

The purpose of this chapter is to present the information obtained from primary sources which is used to analyze and conclude our research.

4.1 Interview Guide

The interview questions came up from the problem definition and theoretical framework. The intention for the specified questions was to provide maximum possible input to the stated problem definition. Questions and interview guide variables are presented in Appendix 1.

4.2 Findings

4.2.1 NCCPL

Respondent: Anosha Aitzed, Information Security Group Head, NCCPL, Pakistan. (For brief facts about company see Appendix II)

4.2.1.1 Operational Risk

According to our respondent from NCCPL, she is information security group head at NCCPL and her team responsibility is to manage any types of information security and operational risks in the organization. Our respondent defined operational risk as it is defined in Basel II (see Appendix 4) which is; operational risk is the risk of losses which comes as a result from poor or failed external events, internal processes, systems and people. She further explained the different areas which are included in operational risk i.e. legal risk, process risk, information technology security, event risk and compliance risk. According to our respondent, generally operational risks are divided into event risks and process risks and it is hard to rank the different areas of operational risks in an organization.

4.2.1.2 Information Risk Management

We came to know from our respondent that how the concepts of information security and risk management are perceived in NCCPL i.e. all about to manage and bound the risks in information confidentiality, availability, authentication, non-repudiation and accuracy.

The respondent further added that to provide the confidentiality in NCCPL, the organization has implemented an information specific framework which uses the instructions related to who is
allowed to enter into the system and who is not. According to her, information risk management is covering three areas which are physical, administrative and technical but the main focus is on technical risk management area. Anosha further said that information risk management is a technical support role with focus on hardware goods and software.

According to respondent, in NCCPL there is a department for information risk management which is called Information Security Group (ISG). Each employee of the organization holds the responsibility of reporting incidents related to Information Technology to a member or group head of ISG. ISG head shall first verify whether the reported incident is occurred or not and is treated according to incident handling policy. As soon as the incident is verified ISG head/member shall notify the incident to manager IT operations. An Employee must not disclose the incident to other employee or any other third party such like customers or vendors.

4.2.1.3 Structure of Organization

According to NCCPL, there is not any separate department for the management of operational risks. Operational risk management comes under the department of information risk management which is called Information Security Group (ISG).

4.2.1.4 Operational Risk and Threats

According to NCCPL, they are dealing with critical operations and therefore they face operational risks everyday in various forms like damage through programming bugs, backup failures, loss of data, inappropriate operational procedures, network damages, unauthorized access etc.

Respondent said it is difficult to rank above mentioned risks because each category has its own importance. For the smooth running of operations in our organization, it is required to pay attention to all risks on equal grounds.

NCCPL has to follow some specific procedures and rules to secure the information as much as possible. In doing so, they have to be very careful even if an employee resigns because he can be a source to leak the information out which can affect on the business of their organization. First of all company will change all the passwords for the resources which were accessible by that particular employee by using password management policy defined by ISG. Then all resources
will be taken back occupied by that person like access card. Meanwhile the backup employee for that person will be activated to take charge of the responsibilities performed by that employee.

Similarly to make the information more secure a framework is being used by NCCPL to protect the confidentiality within the organization. The framework has different policies and instructions about what is allowed and what is not. It is not permitted to use instant messaging and external webmail. There are some specific rules about what type of information can be transfer through allowed communication channels. In order not to bring the company into disrepute, users must apply the same personal and professional courtesies and considerations in Email as they would in other forms of communication.

NCCPL have clear idea that if the information gets leak and confidentiality gets damage, it usually happens because of the deliberate and hard to discover act. It is not possible for an organization to keep the information protected from leakage if the intention of an employee is to really leak the information. If such situation happens then our company can use its legal rights against that person for doing a criminal act.

**Information Accessibility**

When we come to the issue of how NCCPL guard the availability of information, NCCPL as a large established organization has huge resources to put into this significant issue. The organization is continuously improving and planning for the availability of information and to guard the availability of information. One rule in this respect is; the individual who owns some particular information is responsible to define the level of information as confidential, open, strictly confidential or internal. To guard the availability of information from external threats, updated antivirus and firewalls are being used in NCCPL.

**Information Accuracy**

According to respondent, controlling the access is compulsory for any information resource because access gained by an un-authorized object can cause loss of information integrity, confidentiality and availability that may result in loss of revenue, liability, loss of trust, and legal implications to the company. A comprehensive access control policy is implemented in NCCPL which defines who can access what, and covers both physical and logical access to the information resources.
Access control policy implemented in NCCPL identifies various information resources and users, and their boundary in terms of physical and logical access to these resources. It also includes the authentication and authorization procedures for such access.

On the other hand when it comes to secure the information from external attacks, NCCPL uses updated firewalls (FortiGate), configured Access Control Lists (ACL’s) and updated MacAfee Antivirus.

According to respondent, with all these protection policies and rules NCCPL always keeps going to improve its information security system because there are always new challenges every day in technology.

**Information Traceability**

Traceability is being managed in NCCPL by keeping record of each and every action performed by all employees. They have a system to check when, where and how an individual of the organization takes action.

**Standards**

The respondent told us that NCCPL used a recently developed standard called as ISO 27001 to implement information security management system.

**Risks Awareness and Preventive Measures**

NCCPL has defined an access control policy and the scope of this policy covers all information resources present in the company and the users.

When it comes to the point of risk awareness, NCCPL believes whenever there is a failure in any part of the organization, it occurs by a collection of mistakes made by different employees working on different levels. Therefore it is really significant to ensure that all of the individuals working in their organization are aware about their responsibilities and information security risks. All individuals in NCCPL get relevant education in order to ensure the information security awareness within NCCPL.

**4.2.1.5 Management Commitment and Involvement**

The respondent said it is always good to have commitment among employees, in this way employees tend to get the significance of the issues. It is rather straightforward to develop
commitment and involvement from lower level. The top management is more interested in information security and depends on information technology departments to handle those issues. According to Anosha, nowadays commitment is getting more from both, top management and other employees in NCCPL.

4.2.1.6 Impact of operational risks on business

As customers play the key role in the success of a business therefore NCCPL provides various online services to facilitate its customers. NCCPL customers can get information and different services online, for instance settlement services, payment inquiries, transaction inquiries etc. NCCPL has implemented information technology to enhance the functionality and work flow of the organization in order to get success in the business. Information technology enhances the speed of the delivery of products and services, and it improves the quality of services as well.

Respondent explained that, NCCPL considers management, operational and technical controls to avoid the operational risk in order to get the maximum performance for the organization. When this combination of controls is applied properly, it can avoid or bound the damage of an operational risk to a great extent.

4.2.2 CDC

Informant: Waseem Haider, Manager Operation, CDC, Pakistan. (For brief facts about company see Appendix III)

4.2.2.1 Operational Risk

Our representative at CDC briefly defined operational risks as “there are several dimensions of operational risks for instance: market risk, credit risk, political risks and opponent risk”.

According to Waseem, it is quite difficult to answer about what areas are included in operational risks but there are several types of threats which are included in operational risks. These different types of threats can cause a risk. The risk can be defined in a broad manner as internal and external risk.

Informant further explained, despite the fact that it is difficult to define the different areas included in operational risk but all areas have their own significance and therefore they must be
managed in a proper manner. According to respondent as he is manager operations and his responsibility is to manage resources and daily routine operations therefore he is well aware about the fact that if an organization does not pay attention to all areas of operational risk then it will be difficult for a financial organization to carry out their daily operations smoothly.

Informant continued with his job responsibilities and said that he is only responsible for personal level risks in his company. But if some department faces other type of risk for instance; system level risk, unauthorized use or virus attack, so then it is the responsibility of that department to inform about that risk to their Information Technology department where manager IT operations is responsible to manage these problems.

4.2.2.2 Information Risk Management

According to CDC information security includes system security, logical and physical security. Information within a company can be found everywhere like; shelves, computer system and drawers etc. CDC considers standard definition of information security which includes confidentiality, availability, authentication and traceability of data.

Informant further explained about their current information security setup is working fine. It covers all requirements of CDC and no major incident happened because of operational risks in CDC since last three years. Therefore their company is satisfied with current system.

4.2.2.3 Structure of Organization

Respondent said in their organization there is no separate department for managing operational risks. All risks and threats related to information are managed by our information technology department.

4.2.2.4 Operational Risks and Threats

CDC claims that basically there are two dimensions of threats and risks, magnitude and seriousness. It is rather difficult to rank these dimensions, because all are considered very important. Organizations must aware of both manual (personal) and technical (system) risks because both are important areas and these risks can cause serious affects on business.
Inappropriate use of information by people or stealing company specific information constitutes a risk.

According to the question about information leakage, CDC signed several agreements and contracts with its business partners (vendors, employees) regarding to the confidentiality commitments. If any employee resigns from the company, according to company policy, contracts and agreements exist for the employees to protect leakage of information.

CDC manages monitoring arrangements to maintain all emails, internet and all related services that it provides, and the concerned department will apply these monitoring arrangements to all users. Daily internal and external communications via email or instant messaging are monitored through different software’s. It is to be mentioned here that the company does not routinely inspect or monitor email messages but does reserve the right to do so under the prescribed conditions defined in the company’s information security policy. These types of rules are defined in company access control policy i.e. email usage policy and internet usage policy etc. and it is the responsibility of managers of the concerned department to implement policy rules.

**Information Accessibility**

By discussing the availability of information within the company, the main idea is that several employees are well aware about a client business and according to CDC policy every employee has its backup employee, so that in the absence of any key employee, company operations are not affected and the other employee easily takes over the client account. Regarding to the technical perspective, availability of company information is secured by two data centers (one is main site and other one is backup or disaster recover site) and both are synchronous with each other. Several other operators are available to keep the information available for their clients.

**Information Accuracy**

According to our representative, CDC has some rules and policies for authorizations and access of resources. According to resource access policy, every employee is supposed to access those resources and information that he/she needs for his work. It is also important to deny his/her access to those information/resources that are not relevant to their work. Technically it can be difficult to draw lines between rights and authorizations.
Information Traceability

In CDC, every employee has assigned his own username and password to login into the system, when they login into the system, a log gets maintain about their activities and a special auditor group checks the log that whether company policies are followed or not.

Standards

Initially during our interview with Waseem, he got no idea about whether company followed any standard while implementing information security management system or not because his nature of job is not too much technical. But after consulting with his IT department he came to know that CDC didn’t follow any standard during information security management system implementation but they have plan to implement ISO 27001 standard in near future.

Risk Awareness and Preventive Measures

CDC arranges trainings and seminars about the risk awareness after every six months, but according to Waseem, it is only limited for the employees of IT department. According to his opinion, it is best in the interest of the company if they also arrange these types of seminars and trainings for operation department because according to his opinion operation department is on the front line to face these types of operational risks. If employees in operation department are well aware about these threats and risks, they are in a better position to tackle them properly.

4.2.2.5 Management Commitment and Involvement

The board, CEO and management at CDC actively participate and are well aware of issues and problems regarding risk management. They also put effort and time concerning risk management issues but they didn’t involve directly in risk management process. They expect their employees to inform them if the resources regarding risk management process are not sufficient or any major problem occurs during operational activities.

4.2.2.6 Impacts of Operational Risks on Business

According to informant, operational risks on a small level can affect the daily routine activities, such as; in the case of some internal or external viruses or DoS attacks. These are few examples of system level threats which will cause the integrity and confidentiality of data. On the other hand on a large scale operational risks directly affect the business because CDC as a financial
institution holds very critical information regarding to client’s accounts in banks. In operational risks there are some personnel level threats as well, like unauthorized access of data or leakage of information. These personal level risks can cause the organization by damaging its reputation and client’s trust.

According to general risk management approach, risk avoidance is the first step that an organization should try in order to avoid risks before it occurs. CDC applies various methods in order to avoid operational risks. For instance at system level, antivirus software gets updates on daily basis. On the other hand at personal level, access control policies are developed and implemented, appropriate operational procedures are defined to avoid unauthorized access or leakage of information.

According to our discussion about the customer satisfaction, our informant said that, in my point of view customer satisfaction is the backbone of every business because every business (whether it is about to provide product or services) is designed for customers.
5.0 Analysis

*The focus of this chapter is to analyze the secondary information presented in theoretical framework and primary information presented in empirical findings.*

5.1 Operational Risks related to Information Security

As it is cited in the literature, operational risk includes personal risk, organizational risk, change management risk, portfolio risk, country risk, reputation risk, legal risk, currency risk, business continuity risk, strategic risk, and shift in credit rating, taxation risk, and regulatory risk (Hussain, 2000). However, according to findings few of these areas which are legal risk, process risk, information technology security, event risk, and compliance risk included in operational risks. On general basis operational risk can be defined as a residual risk (i.e. every risk except market or credit risk) (Marshall, 2001).

The specified definitions are quite broad. To explain these definitions in more detail, literature further explains operational risk as a process of procedures, systems, policies, and expertise (Hussain, 2000). According to findings, in NCCPL operational risk is defined as a risk of losses which comes as a result from poor or failed internal processes, external events, people and systems. On the other hand in CDC operational risk is defined as a result of direct and indirect losses which occur because of human errors, external events, internal routines, and inaccurate systems.

According to findings operational risk occurs because of internal problems and environmental factors. Saunders (1998), external and internal approach used the same way to divide the risks. According to O’Brien et al (1999), operational risks are divided into two categories which are operational failure risk and operational leverage risk. Operational failure risks occur due to internal factors and operational leverage risks occur due to external factors. It is found from the findings that the way interviewees divide the operational risk follows the approach given by O’Brien et al (1999).

But on the other hand, Bessis (1998) divided the operational risks into two levels consisting of technical issues and organizational characteristics respectively, which is a different way as compare to the findings. Technical issues and organizational characteristics are considered as
part of operational risk but the division of operational risks into this specific way is not done by any other author.

To summarize, both financial organizations almost have the same perception about operational risks but different authors have different opinions about operational risks. After analyzing the secondary and primary information we found an approach given by Elke (2003) most reasonable in which Elke divided the operational risk into two categories; external risks and internal risks. Elke (2003) further divided the internal risks into three categories which are system risks, process risks, and personal risks.

5.2 **Impact of Operational Risks on Business**

Customer satisfaction is the key objective in financial organization. Therefore both financial companies NCCPL and CDC have given the platform to their customers to perform different online tasks for instance internet banking and according to (Lachello, n.d.) providing online services involve many types of operational risks. Though organizations provide online services to facilitate their customers but it increase the probability to lose the information (Solms et al, 1998).

Since the information in financial organizations is very critical so it can severely affect the business of a financial organization. As (Philip, 2009) there are several types of risks which can affect the business of a financial organization but operational risks are considered the most important type of risks because these type of risks can not only harm the business of an organization, these risks even can destroy the business.

There are many financial organizations where business got severe affects from operational risks. For instance operational risks demolished a financial organization named IPremier because IPremier did not implement any risk management plan to manage operational risks. Austin stated that business of IPremier get demolished because there was no risk management plan to prevent, resist and recover the virus attacks (Applegate et al., 2007, pp. 369).

According to the findings, interviewees stated that as their organizations are dealing with critical operations therefore NCCPL and CDC face operational risks every day. However operational risks occur in different forms like, backup failures, operational procedures, unauthorized access,
and loss of data etc. These operational risks differ in their intensity. Some of these operational risks can affect the daily routine activities, some of them can affect the confidentiality and integrity of data, and some of them can even destroy the business. Findings depict that NCCPL and CDC are well aware of the importance of operational risks and following different techniques and polices in order to avoid operational risks therefore NCCPL and CDC did not get any severe incident so far due to operational risk.

Concluding the issue we could say that organizations should take security threats seriously and should develop the appropriate risk management plan because successful strategy and risk management plan could make the difference between the organization’s continued existence and sudden death.

5.3 Top Management Involvement and Commitment

Top management plays an important role in information risk management (Hussain, 2000). The views of Kotulic and Clark (2004) are almost same like Hussain; they state significance of the top management’s role and their responsibility in managing information system. Top management should assure that culture, systems, structure of the organization and people are contributing to effective information risk management (Kotulic & Clark, 2004). According to the findings, top management in CDC and NCCPL which includes Chief Executive Officer (CEO), Chief Operating Officer (COO) and Chief Technical Officer (CTO); they all are actively participating and are well aware of the issues related to risk management.

According to Shimpi (1999), many people in an organization put their efforts to increase the profitability of their organization, but when it comes to the point of risk management a few of them put their efforts in this regard. It is therefore interesting to know about who are the concerned persons for establishing the strategy of risk management. Our respondent at CDC said, although the top management put their time and effort but they don’t get involve directly in risk management process, whereas in NCCPL, top management helps and provides required resources to staff in order to enhance information security.
5.4 Solutions to enhance Information Security

There are various techniques which can be used to enhance information security for instance access control policy, email usage policy, internet usage policy, password management policy, system usage policy, incident usage policy, information security standards etc. But access control technique is considered as the most significant technique in order to secure information (Zhongping et al., n.d.). Different authors defined the concept of access control in comparatively similar ways. Hagen et al. (2007) state that an organization must have a system that specify who can get access to a particular piece of information. From the findings authors found that NCCPL and CDC are well aware of the significance of implementing access control policy and hence both financial organizations have implemented comprehensive access control policies with the purpose to restrict the access of resources in order to enhance information security. Access control is a policy which assures that the requests from authenticated users will be accepted and from unauthenticated users will be rejected (Zhongping et al, n.d.). Organizations can avoid many types of risks in order to improve their information security by implementing right access control measures (Hagen et al., 2007, pp. 4-6).

There are four possible approaches to manage risks which are risk avoidance, risk reduction, risk transfer, and risk retention. As risk avoidance and risk reduction minimize the organization’s overall exposure to risk therefore these approaches are considered as risk control approaches (Shimpi, 1999). On the highest priority financial organizations must try to avoid the risk because Herold (2005) states in his book, “prevention is much less expensive than response and recovery”. Empirical findings also suggest that a financial organization must use preventive measures. One from our two respondents said, as we are dealing with critical operations so we always use preventive measures to avoid the risk. The respondent further stated that there is an Information security Group who is responsible for developing and implementing these polices and measures.

Another step in the process of enhancing information security is to implement Information security management system (ISMS). If ISMS is implemented properly it will help the organization to provide information to only right people. According to Eloff and Eloff (2003), ISMS deals with all aspects of an organization which are significant in creating and maintaining
a secure information environment. The process ISMS encourages the use of standards which plays significant role to enhance information security. According to Humphreys (2006), ISO/IEC 27001 standard was developed to secure the information assets of all types of organizations. Our respondent from NCCPL said that in their organization ISO 27001 standard has implemented in order to enhance their information security environment. But on the other hand the findings depict that CDC did not follow any standard while implementing information security management system but they are convinced that they will implement ISO 27001 standard in near future to enhance information security.

According to the findings, NCCPL has implemented a framework to improve information security. The implemented framework consists of various instructions and polices about different access rights for different persons to make it sure that every person is restricted to his rights only. Further the implemented framework restricts the employees by not allowing them to use instant messaging and external webmail. According to Saran & Zavarsky (2009), though email services are not considered secure means of communication and these services can be used improperly therefore an organization can use email usage policy to encourage the proper use of email services. Saran & Zavarsky (2009) further state that internet usage policy can also be used to establish rules in order to educate the individuals about the correct usage of internet.

It was quite interesting to know that when NCCPL does not allow its employee to use instant messaging and external communication where CDC allows its employees to use all communication ways by means of instant messaging, internal communication and above all external communication. Though CDC allows all ways of communication but then communication is being monitored using different software’s.

“Risk management is not a onetime process; it is an ongoing activity” (Olzak, 2007). Through our empirical study, we came to know that the target companies of our research work are almost using the same approaches but there are little bit deficiencies in implementation. With all these protection policies, standards and rules, the financial organizations always keep going to improve its information security system because they always face new challenges every day in technology.
<table>
<thead>
<tr>
<th>Sr.no</th>
<th>Operational Risks</th>
<th>Effects on System/Services</th>
<th>Affects on Business</th>
<th>Appropriate Solutions/Control Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Programming bugs/virus attack</td>
<td>Data damaged or loss of data</td>
<td>Directly affect on business as financial institutions have critical data</td>
<td>Firewalls, VPN Tunnels, ACL’s, antivirus solutions</td>
</tr>
<tr>
<td>2.</td>
<td>Backup failure</td>
<td>Data unavailability for users</td>
<td>Customer’s dissatisfaction/affects on business</td>
<td>Every device has proper backup, should be updated with main devices on monthly basis</td>
</tr>
<tr>
<td>3.</td>
<td>Inappropriate operational procedures</td>
<td>System problem, data unavailability, leakage of information</td>
<td>Might cause information leakage that affect company’s reputation</td>
<td>Define password management policy, email usage, internet usage, computer usage policies</td>
</tr>
<tr>
<td>4.</td>
<td>Unauthorized use</td>
<td>Leakage of information</td>
<td>Business financial loss, affect company reputation, customer dissatisfaction</td>
<td>Access control policy in which access of each personal is defined against each resource</td>
</tr>
<tr>
<td>5.</td>
<td>Workflow interdependencies</td>
<td>Delay in services</td>
<td>Customer dissatisfaction creates affect on business</td>
<td>Define appropriate operational procedures</td>
</tr>
<tr>
<td>6.</td>
<td>Dependency on external personnel (Vendors)</td>
<td>Delay in services/data stealing threat</td>
<td>Customer dissatisfaction creates affect on company reputation</td>
<td>Signe proper agreement with vendors for smooth running of services</td>
</tr>
<tr>
<td>7.</td>
<td>Network damage/power problem</td>
<td>System not available for users</td>
<td>Customer dissatisfaction creates affect on business</td>
<td>Alternate communication links and power systems like UPS/Generator</td>
</tr>
<tr>
<td>8.</td>
<td>DoS Attacks/ Hacks</td>
<td>Services not available for clients/data stealing/modification of information in wrong way</td>
<td>Affect company reputation, customer dissatisfaction, business financial loss</td>
<td>Update network equipment, define incident handling policy, maintain recovery procedures</td>
</tr>
<tr>
<td>9.</td>
<td>User error</td>
<td>Modification of information in wrong way (intentionally or unintentionally)</td>
<td>Affect company reputation, customer dissatisfaction, business financial loss</td>
<td>Maintain logs against each user account, define legal rights policy</td>
</tr>
</tbody>
</table>

*Table 2: Operational risks, solutions and impacts on business, Source: Authors*
6.0 Conclusion

The purpose to write this chapter is to wrap up the analysis and findings in order to provide the answers of the research questions.

Operational risk from a business perspective is most commonly defined as a risk which comes through the production of goods and the services given to the clients of a financial organization. During our research, we found that different authors have defined different types of operational risk related to information security. But after analyzing we conclude that operational risks related to information security in a financial organization are virus attacks, backup failures (loss of data), inappropriate operational procedures, unauthorized use, and dependency on external personnel such as vendors, user error, network damages, and destructive hacks such as Distributed Denial of Service attacks.

One of the main motivations to underlie this research was to boost the financial organizations to follow the efficient and effective procedures in order to reduce the probability of operational risks. Since high probability of operational risks can affect the business to a great extent. As we have seen earlier that many financial organizations experienced huge losses in their business because those organizations were not able to properly manage their operational risks. These operational risks can cause a financial organization to have financial losses, reputation losses or even operational risks can demolish the business of a financial organization. Therefore to gain success in the business, financial organizations need to reduce the exposure of the operational risk.

In the beginning of our research, we assumed that top management is not intricate in the process of operational risk management and information risk management. But after pinning down the analysis we conclude that top management is well involved and committed concerning these processes. They are well aware of the fact that no financial organization can get success in the business if they don’t show their commitment and interest in order to reduce the exposure of operational risk related to information security. So, to reduce the exposure of the operational risks related to information security, top management show their interest in adopting new ways and policies to enhance information security. Based on our research work we are able to conclude that there are various techniques which can be used to enhance information security which are access control policy, email usage policy, internet usage policy, system usage policy,
password management policy, and incident handling policy. A financial organization can use these polices in order to minimize operational risks and to enhance their information security management system.

The industry of operational risk management is growing because operational risk management is still immature. Through creating a culture of awareness for operational risk management, financial organizations can enhance their abilities in order to attain their objectives, to improve the technology, and to improve the efficiency of the processes. It would lead financial organizations to get higher profits, minimize losses, and enhanced customer satisfaction.
7.0 Recommendations

After analyzing and concluding the research, some recommendations are presented in this chapter for financial organizations which can be used to avoid Operational risks and improve the current system of information security.

In order to decrease the probability of operational risks and to enhance information security, it is recommended that any information that users consider sensitive or vulnerable should be encrypted. The passwords should be kept secured and user accounts should not be shared. Authorized users should be responsible for the security of their passwords and accounts. User and system level passwords should be changed frequently.

For the sake of maintaining privacy and confidentiality, installing desktop sharing tools and software on any of the company resources should not be allowed. Only necessary and licensed software and applications should be installed on the machines. Unwanted and unauthorized software should be removed from the machine. The user should follow a formal procedure if there is a requirement of new software which is not on the approved list of software maintained by the company. Every workstation should be equipped with the best available antivirus software and the virus definition files should be kept updated at all times. Every workstation should be kept updated with the latest operating system patches and updates.

Employees must be careful when e-mail attachments are received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.
References


**Personal Communication**

Personal interview with Anosha Aitzed; Information Security Group Head- NCCPL (Personal communication, April 28, 2010)

Personal interview with Waseem Haider; Manager Operation- CDC (Personal communication, May 06, 2010)
APPENDIX I

Interview Guide Variables

Some areas of discussion are defined below with logical reasoning to ask questions during interview session.

Operational Risk

The purpose for asking questions related to operational risk is to get an understanding for the different domains of risk, and to find out whether information risk is a part of operational risk or it is counted as a risk of its own.

Information Risk Management

While studying the literature, we got various unclear definitions related to information risk management. To make our understanding and knowledge better we asked for definitions related to information security risk management to the respondents.

Structure of Organization

In order to improve our understanding about information risk management, we thought it is significant to put questions which are concerned about how the work in the domain of risk was formed and structured.

Operational Risks and Threats

The purpose to ask questions related to Operational risks and threat was to find out the threats that form an operational risk for a financial organization. In order to conclude that how the different financial organizations perceive operational risk, we wanted to know the character of those threats and risks; whether those risks and threats were of technical character or organizational character

Management Commitment and Involvement

The purpose for asking these questions was to figure out that how much top management is committed and involved in information risk management. We were also interested to figure out
that, is there any difference between awareness and involvement of top management and other employees.

**Interview Questions**

**Operational Risk**

1. How would you briefly define operational risks?
2. Which areas are included in operational risks?
   2.1. At which area operational risks mostly occur?
   a. Personal processes
   b. IT/ systems
   c. External Processes
3. Is it you who take the overall responsibility of managing operational risks in your organization?
   3.1. If yes, what is your job title?
   3.2. If no, then what is your designation?
   3.2.1. Who is responsible and what is his designation?

**Information Risk Management**

4. How would you define the concept of information risk management?
5. Which areas do you think the concept of information risk management covering?
   a. Administrative
   b. Physical
   c. Technical
6. Information risk management could be defined as any of the following, which do you think is most consistent with your image of the concept?
   “Information risk management is a technical support role, focusing on hard goods and software”
   OR
   “Information risk management is an operational function that focuses more profound over the availability, integrity, accuracy and confidentiality of information”
7. How risk management is being managed in your organization?
8. Does the existed risk management system solve threats and risks properly and are you satisfied from it?
   8.1. If not, why not?
      8.1.1. What do you think, what changes should be there in the existed risk management system to enhance information security?

**Structure of Organization**

9. Do you have a separate department for the management of operational risks related to information security in your organization?
   9.1. If yes, what specifically it is called?
      9.1.1. What does the department do? (If a risk is discovered)
      9.1.2. Who is responsible for this department?
      9.1.3. How many people are working in this department?
   9.2. If not, why not, what are the issues in establishing a separate department for this domain?

**Operational risks and threats**

10. What are the operational risks to information in your Company?
11. What type of risk you consider most important to manage?
    a. Leakage of Information
    b. accessibility to information
    c. modification of information in the wrong way
    d. traceability
    e. other risks and threats
12. If an employee resigns, how can the organization keep the information consistent that he has been protected? (Confidentiality)
13. What guidelines are there for the daily internal and external communications? (Send information via email, instant messaging)
14. How do you prevent employees to take the information to their homes? (Customer lists, information on other dept)

**Information Accessibility**

15. What procedures and policies do you follow to guard the availability of information? (e.g. if a key person is sick or disappears or his computer explodes)
Information Accuracy

16. What are your rules for who has access to the information and who has not?
17. What is your protection policy for external attacks? (Firewalls)
18. Do you have any intention to enhance the information security?

Information Traceability

19. How can you track who did what at what time with some information?

Standards

20. Did your organization follow any standard while implementing information security management system?

Risk Awareness and Preventive Measures

21. How to allocate resources in the different parts of the Information Risk Management?
22. How do the employees in your organization know about the information security operational risks? (Risk awareness, risk culture)

Management Commitment and Involvement

23. How much top management is committed and involved in issues of operational risks related to information security?

Impact of Operational Risks on Business

24. How operational risks affect the business of your organization?
25. What procedures do you follow to avoid operational risk?
26. Do the customers get affects by the operational risks?
APPENDIX II

Brief Facts about NCCPL

Pakistan’s Capital Market consists of Depository Company, stock exchanges and NCCPL. National Clearing Company of Pakistan Limited (NCCPL) is an institution of Capital Market in Pakistan which provides settlement and clearing services to all stock exchanges in the country.

The company was formed in 2001 to manage the National Clearing & Settlement System (NCSS) in a complete automated electronic settlement system. The company became operational in 2003-04.

For further details about the company please visit the company website http://nccpl.com.pk/about_us/ (Accessed on 28\(^{th}\) April 2010)
APPENDIX III

Brief Facts about CDC

Central Depository Company of Pakistan Limited (CDC) is the only one depository in Pakistan. The company was formed in 1993 as a public limited. The company became operational in 1997. CDC is handling the electronic settlement of transactions carried out by all stock exchanges of Pakistan.

CDC is providing depository services to various Capital Market participants who include Asset Management Companies, Brokers, general retail investors and Banks.

The purpose of CDC is to functions as a central securities depository on the behalf of financial services industry to contribute to the Pakistan's ability to support an effective capital market system that will attract retail level investors and institutional from abroad and Pakistan.

For further details about the company please visit the company website

http://www.cdcpakistan.com/UserPanel/AboutUs/ViewContent.aspx?m=au&type=0001

(Accessed on 04th May 2010)
APPENDIX IV

Brief Facts about Basel II

Basel Committee was established by central bank governors of Group-Ten countries in 1974. It has about 30 task forces and technical working groups. The members of Basel committee are from various countries like Italy, France, Belgium, Japan, Canada, Spain, Luxembourg, Sweden, the Netherlands, United States, Switzerland, and United Kingdom.

In 1988, Basel committee decided to introduce a new capital measurement system which is commonly referred to as the Basel Capital Accord, termed as Basel I. Later in 1999, Basel committee proposed Basel II to replace Basel I. Basel II consists of supervisory review of an institutions internal assessment process, minimum capital requirements, and effective use of disclosure to strengthen market discipline. In Basel II, operational risk is defined as “the risk of losses resulting from inadequate or failed internal processes, people and systems, or external events”.

For further details about Basel II visit following website

www.bis.org

(Accessed on 15th April 2010)