Open University Cyprus **Hellenic *Open University***

Master's join degree/post graduate Program
Enterprises Risk Management (ERM)

MASTER THESIS

Operational Crisis Management and the Influence of Cyber – Threats and External Fraud to Business Continuity Planning in International Banking Industry

Chrystalla Venizelou

Supervisor:
Dionysios Gerontogiannis

May 2018

Open University Cyprus **Hellenic *Open University***

Master's join /post graduate Program
Enterprise Risk Management (ERM)

Master Thesis

Operational Crisis Management and the Influence of Cyber – Threats and External Fraud to Business Continuity Planning in International Banking Industry

Chrystalla Venizelou

Supervisor:
Dionysios Gerontogiannis

This Thesis submitted for partial fulfillment of the requirements
Master's join degree/post graduate programme
«Enterprises Risk Management (ERM) »
Faculty of Economics and Management

Open University of Cyprus **Hellenic Open University**

May 2018

Blank Page

Summary

The purpose of this study is to presents a comprehensive presentation of one of the most popular risks facing the international banking sector every day, the Operational Risk.

This research consists of two parts, a thorough literature review and a survey. A the first part is studied the Operational risk management, operational risk factors, operational risk management in banking sector, categories of operational risk in banks, cyber threats and external fraud, operational risk and business continuity planning. At the second part of this master thesis follows a qualitative and quantitative analysis of the collected data. In the survey participated bank employees from different departments and position. The purpose of this survey is to interpreted and discussed to address the operational risk of cyber threats and external fraud in the banking industry to classify the impact of cyber threats and external fraud as factors for a crisis in the banking sector with a malfunction planning the continuation of activities. Another objective of this study is to identify the importance of operational risk assessment in the banking sector.

The results of this research shows that the factors of people and processes affect the Operational Risk. Further, Cyber risk has strong negative linear relationship with Incompetence, on the other hand, External Fraud has no relation with Incompetence, low morale, high staff turnover. External Fraud has strong positive linear relationship with the factor Fraud which includes for example the hackers and with Money Laundering. From the results was presented a significant relationship between Operational Risk, External Fraud and Cyber Risk, with Business Continuity Planning which concludes that an Effective Business Continuity Planning can result a better addressing of the External Fraud and Cyber Risk that bank deals with.

Acknowledgements

Firstly, I would like to express my gratitude to my thesis supervisor Dr. Dionysios Gerontogiannis of the Faculty of Economics and Management of Open University of Cyprus for his contribution, constant guidance and support

I would like also to express my appreciation to the faculty members of Open University of Cyprus, Dr. Michiotis, Dr. Koutsoukis, Dr. Agiomirgianakis and Dr. Ipsilandis. The knowledge they transfused to me was a valuable asset for the completion of my thesis.

Finally, I would like to thank you my family, friends and colleagues for providing me with support and continuous encouragement throughout my studying and during the process of researching and writing this thesis.

Thank you.
Chrystalla Venizelou

Contents

Appendices

Chapter 1
Introduction

1.1. Study Background

The risk management process can be defined as a systematic procedure of management strategies, creating the context via the processes and identifying, analyzing, assessing, treating, monitoring and communicating risks (Cooper et al., 2005). The second stage of Risk Management process, which is one of the most important stages of this procedure, Risk Assessment is used to analyze the potential risk from the collected data. When you evaluate and estimate the levels of risk which are involved in a situation, comparing against benchmarks and determination of an acceptable level then this is the definition of the risk assessment (ISF, 2010). Risk assessment follows the risk identification and its purpose is to evaluate how big the risks are, pay attention to the most important threats and opportunities, to measuring and prioritizing risk (COSO, 2004).

One of the most important risks that a bank is dealing with is Operational Risk. *In the financial institutions, the operational risk is differentiated from the other risks because you measure this risk in terms of potential economic losses (Hopkin, 2010). It is very important to managing operational risk to all business environments. Operational risk has been defined as the risk that will interrupt normal everyday activities. Two of the most significant operational risks in banking sector, especially the last decade, is cyber threats and external fraud due to the globalization and digitalization of the banking environment. Most of the banks in order to effectively deal with these risk incidents, they use the business continuity planning as part of their risk management process.*

1.2. Problem Statement

The most significant components of a risk management system are to identify and defining the risk, assessing and mitigating the risk that enterprises are exposed to. In this dissertation will study the Operational Crisis Management in the Banking Sector which is one of the most crucial and everyday risks that banks dealing with. Furthermore, we will deal in depth with the two most important operational risks for 2017, Cyber threats and External Fraud, the factors connected to those risks and the impact on business continuity. Cybercrime and external fraud are emerging as a challenge for security in the international banking sector. This thesis aims at providing more understanding of cyber risk and external fraud, with emphasizes in risk assessment. Risk assessment provides a comprehensive model that can be applied in identifying the methods through which cyber threat and fraud are committed, avoiding further risk activities occurring and providing guidelines of handling those events and acting against perpetrators.

1.3. Research Objectives

This research is to review the Operational Risk Management in the International Banking Sector and to classify the impact of cyber threat and external fraud to business continuity planning and also the importance of risk assessment in Operational Risk Management in the banking sector.

1.4. Research Questions

- To find out which are the factors connected with Operational Risk of cyber threats and External fraud in International Banking Industry
- To investigate how the cyber threat and external fraud influence as factors for a crisis in the banking industry with malfunction at the business continuity planning
- To explore which are the risk assessment methods and what are the advantages and disadvantages of each method of the operational risk assessment in the banking sector.
- To summarize findings and make recommendations

1.5. Brief Overview of Methodology

Questionnaires were administered to Bank Employees and interview schedule used to collect information on the Operational Risk Management process. Simple Random Sampling used to administer the questionnaires to ensure statistical conformance. Data collected was analyzed qualitatively and quantitatively, using SPSS as well as Microsoft Excel.

1.6. Problems and Limitations of the study

The survey presented to preconception and prejudice to the respondents. Therefore, 100% accuracy cannot be ensured. Other major limitations come across include, the difficulties associated with data collection, study design and sampling techniques as well as size, as for instance, respondents failed to return completed questionnaires on time, citing time constraints and work pressure as some of their reasons. Also, this study limited to the observations conducted in International banks.

1.7. Significance of this study

The present study is intended to show an integrated presentation in one of the most popular risk where international banking sector has to tackle on a daily basis. We will focus on two categories of Operational Risk, Cyber Threats and External Fraud, and related factors as well as how they affect business continuity of international banking industry. This study would help other researchers to demonstrate the theory and also support the future research, produces good ideas and also delivers better understanding.

Moreover, this study aims to provide a practical guidance on best practice in regard to an effective way of operational risk assessment in banking sector. It will further contribute to build knowledge on methods used to assess operational risks, the area of operational risk assessment, provide suggestions to the improvement of the operational risk assessment in the banking system.

Blank Page

Chapter 2
Literature Review

In this chapter, we will develop a conceptual framework of the main subjects of the research: Operational Risk Management, Cyber Threats and External Fraud, Business Continuity and Risk Assessment. The purpose of this chapter is to survey the recent literature on operational risk in banks. In the beginning we going to define the risk management and the types of risk in the banking sector. Then the chapter continues to define operational risk which is the essential theme of this study, and then it continues to examine the influence of cyber threats and External fraud in the banking sector. Furthermore, this chapter will discuss the characteristics of operational risk process and business continuity.

2.1. Risk Management

The risk management process is a systematic procedure of management policies, establishing the context via the processes and identifying, analyzing, assessing, treating, monitoring and communicating risks (Cooper et al., 2005). Thus, for understanding and managing risks in a project you need to use the risk management process. According to Osborne (2012) one of the most important part of any organization's strategic managing is the risk management. With this application organizations can methodically address the risks connected with their activities to accomplish their objectives. Risk management pays attention to the identification and treatment of these risks. The goals are to add maximum sustainable value to all the activities of the organization. Recognize all the factors that affects the organization's objectives and increases the likelihood of success and decrease the probability of failure and uncertainty (Osborne, 2012).

Moreover, Osborne (2012) stated that the people involved in risk management they have a negative point of view of the risk and they believe that many risks

have negative consequences. On the other hand, as per Osborne, many risks have positive consequences. Consequently, Organizations can grow and flourish by establishing an effective risk management with focus on reduce the negative and increase the positive consequences of risk.

Another definition of risk management is the one of Ozturk (2007) who says that risk management which is a procedure for taking a risk which satisfy the managers. This procedure includes the identification of key risks, achievement of understandable, operational, reliable risk measures, choosing which risks to rise and which one to decrease and the way it must be achieved.

Furthermore, managers should be able to establish procedures so that they can monitor the risk. This means that risk assessment phase in risk management evaluate of dangers associated with a specific position by measuring its magnitude and justifying such exposures to achieved the institutional goals (Awojobi.et al, 2011).

The Committee of Sponsoring Organizations of the Treadway Commission (COSO, 2004), defines ERM as follows: "Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives" (Committee of Sponsoring Organizations of Treadway Commission,2004, p.2)

Smith et al. (2006) comprehensive approach on risk management considers risk management as a tool that helps taking better decision, by knowing the information from the investment. This has as a result, when the information that managers get are insufficient then they do not need to make any decisions and this will lead to better overall performance.

Cooper et al. (2005) describe the risk management concept as:

“The risk management process involves the systematic application of management policies, processes and procedures to the tasks of establishing the context, identifying, analyzing, assessing, treating, monitoring and communicating risks” (Cooper et al., 2005).

2.1.1. Risk Definition

Risk is being defined by the Oxford English Dictionary as “a chance or possibility of danger, loss, injury or other adverse consequences’ and the definition of at risk is ‘exposed to danger”.

The Institute of Risk Management (IRM) defines that the combination of the probability of an event ant it's consequences, positive and negative, is a risk.

Risk is defined by the Institute of Internal Auditors as the uncertainty of an event that impacts the objective's achievement. Further, Institute of Internal Auditors said that we can measure risk based on consequences and likelihood.

In an organizational environment risk is defined as anything that can impact the accomplishment of company's objectives. Risk is a multifaceted and not always simple meaning. In ancient Greek and Italian, they used to use the word risk in uncertain situations and it destined "to dare" (Hamberg, 2000, Picket, 2013). Hence, people and business should be trying to carry out their goals even if the there is a risk situation with unexpected outcomes since risk is unavoidable (Kaplan & Garrick, 2006). Hamberg (2000) believes that in in risk events the probability of outcomes is known although in uncertain events the outcome are unknown. Moreover, risk can involve some loss or damage (Kaplan & Garrick, 2006). Additionally, a situation can be considered as risk in each time, but maybe in the future not be consider as a risk (Cornia, Dressel & Pfeil, 2014).

According to Andersen and Terp (2006) risk can been defined as internal and external events, uncertainties or circumstances which a company should effectively recognizes and manage to fulfill the company's goals and create shareholders value.

2.1.2. A Concept of Risk Management

For understanding and managing risks in project the use of Risk management process is fundamental. The main phases that risk management consists are: identification, assessment and analysis, and response (Smith et al. 2006). To have an efficient process all steps of risk management process should be included when dealing with risks.

Risk management is: "A process of understanding and managing the risks that the entity is inevitably subject for achieving its corporate objectives. In management, risks are usually divided into categories such as operational, financial, legal compliance, information and personnel. One example of an integrated solution to risk management is enterprise risk management." (CIMA Official Terminology, 2005, p. 53).

In Finance and Investment sector, the most important component for success is risk management. A combination of effective risk management and corporate governance is needed for the confrontation of the Global Financial Crisis (Aebi, Sabato & Schmid, 2011). If Companies adopting risk management practices and having appropriate risk management strategy, they will have the opportunity to increase the likelihood of long term survival (Kim & Vonortas, 2014). Board of directors and senior executives and employees in any position should understand the risk management process. There are three main factors where risk management strategies are concentrating: following to control-based objectives and complying with regulatory requirements, meeting or exceeding an organization's objectives, (COSO, 2013). Moody's study (2010) find out that the risk management process should be part of organizational processes and decision making though it should be dynamic and responsive to changes, to increase the effectiveness of risk management in the organization. Risk management confirms that the process of identifying, measuring, controlling/monitoring and reviewing is applied through the entire risk management process for the organizational goals set by the board of directors. In addition, the board should be aware of the risks and the management plan. Furthermore, a chief risk officer there must be in the company for ensuring that

the risk management process is executed correctly. The main responsibilities of chief risk officer is to asserts that all risks are strategically evaluated within the corporate risk policy, the company is responding properly to new risks and challenges, and provides advice on sensitive risk issues for appropriate decision-making (Picket, 2013). Another responsibility of chief risk officer is to implement an internal control system effectively for managing the risks efficiently. Nevertheless, chief risk officer should understand some obstacles that may occur such as insufficient strength of the process, insufficient risk managers, unsuitable risk analysis and inacceptable attitude when assessing the risk management plan (Carter & Chinyio, 2012).

2.1.3. Benefits with Risk Management

Risk management process is an ongoing procedure during the entire project to maximize the efficiency of risk management, thus risks will be discovered and managed through all the phases (Smith *et al.* 2006). Some of the benefits of risk management are to help recognize the possible costs from unmanaged risks and the how to avoid them (Thomas, 2009) and to increase the level of control thru the project and the more effective processes for solving the problems, it analyses the project conditions from the beginning (Perry, 1986). Possible and sudden surprises can be reduced from the risk management procedure (Cooper et al. 2005).

2.1.4. Limits of Risk Management

The project complexity is related with the level of risk (Darnall and Preston, 2010). The bigger the project is, the larger the number of potential risks that may be faced. There are several factors which can induce risk occurrence. The most common factors are financial, environmental, time, design and quality. Another factor that influence the occurrence of risk are the technology used and the organization's risks (Gould and Joyce, 2002).

According to Cleden (2009) complexity can be a factor that can limit a project, if the complex of the project is big then more resources are require to be completed Moreover, the project team should always remember that even if the

potential risks were identified there always a possibility more threats to be appeared. Consequently, the project team should always be alert for any new potential risks which might arise and not be only focus on management the identified risks (Cleden, 2009).

2.2. The Risk Management Process

A systematic process of identifying, analyzing, evaluating, treating and monitoring responding to risks can be defined as Risk management (Dey, 2010, McPhee, 2005). This is a proactive and continuous process which identifies discrete risks, assesses the likelihood and consequence of these risks, develops mitigation options for all the identified risks, monitors progress to confirm that the risk is declining (DoD, 2017). Risk Management includes the preparation for potential risks that can happen unexpectedly and solving problems too. According to Winch (2002), by managing the potential threats has as a result to minimize losses and it is also a way to transfer risks as opportunities, that can lead to economical profitability, environmental and other advantages (Winch, 2002).

Risk management includes all activities that permit the probability of risk occurring or its effect to be eliminated or reduced (Pálinkás 2011). The risk management contains four main steps:

- Risk Identification
- Risk Assessment/Analysis
- Risk Control
- Risk Monitoring

The first step of Risk Management is the identification of risks which is the process of identifying threats that may have an impact on the goals of the organization and also it could be about the opportunities (Crouhy M., Galai D. and Galai Mark, 2005). For an effective risk identification, the use of several instruments it is very important. The instruments that using for the performed of risk identification are: insurance policy checklist, risk analysis questionnaires,

flow process charts, analysis of financial statements, inspection of the firm's operations (Vaughan, 1997), checklists, documentation review (Denizand Kaymak, 2007), brainstorming (Chapman, 2001), surveys (Bajajetal, 1997),interviews(Chapman, 2001),strength weakness opportunity threat (SWOT) analysis (Sweeting, 2011), nominal group technique (Delbecqand Vande Ven, 1971),and Delphi technique(Chapman, 1998). The next step is the Risk assessment//Risk Analysis which involves the evaluation of the probability and the consequences of a risk event when it occurs. Furthermore, with Risk analysis we are gathering and assessing information about risk exposure, so that the organization to take the correct decisions and manage risk properly. Hence, the assessment step includes measuring the potential size of the loss and the likelihood, classify the risks according the priorities of organization. Therefore, the risk assessment step would provide important information which an organization should pay attention on certain risks Nevertheless, any failure in risk assessment may be costly and creates delays (Serpella et al. 2014). If the identification process is reliable then this ensure that the risk assessment will be effective (Tworek 2012; ISO 2009).

The third step in the risk management process, is the Risk Response which is about the techniques or strategies that should be used to handle each risk. The most common strategies used are avoidance, reduction, retention, and transfer (Cienfuegos, 2012). Finally, risk control includes the ongoing monitoring of the identified risk, risks assessed and risk control processes and reviewing them to make sure they are working efficiently (Crouhy M., Galai D. and Galai Mark, 2005).

2.2.1. Risk Identification

Risk identification is the first step of risk management process, which is informal and can been performed in different ways, depending on the organization (Winch, 2002). Past experiences, allocating potential risks are factors that risk identification depends on them. After identified the risks it is easier to take actions and control them. When the causes of risk are identified and allocated

before the problems occur then we have a more efficient risk management procedure (PMI, 2004).

The main goal of identifying risks is to create a list and highlight the potential risks should a company to be managed (PMI, 2004). Moreover, Risk identification is a key step in the risk management process, aims to identify potential risk that may affect the accomplishment of its objectives, identify the source of the problem, analyzing the problem (Spedding, Rose, 2008). Risk identification process includes risk-ranking mechanisms which are based on impact (Barton et al., 2002). Barton et. all (2002) said that the analysis helps to categorize the risk based on the importance and helps the organization to develop efficient risk management strategy.

This step includes not only the identification of the possible risk but also the identification of the possible causes of the risk event. The causes of the risk can be more than one, which directly or indirectly contribute to the risk event occurring. Determine the causes can be helpful to understanding the risk, identify controls, evaluate the existing controls, and create an effective risk treatment (Western Australia Government, 2011). Effective risk management dependent to correct risk identification. If risk managers do not succeed in identifying all possible risks that challenge the organization, then this is costly for the organization and the risks that cannot be identified are becoming non-manageable (Greene and Trieschmann, 1984).

Tchankova (2002), said that risk identification involves four elements: sources of risk, hazard factors, perils and exposure to risk. Sources of risk include the elements of the organizational environment that can bring negative or positive outcomes. Hazard can increase the possibility of losses or gains. The term "Peril" is something that is close to risk and it has negative, non-profitable results. Last, Resources exposed to risk are objects facing possible losses or gains.

Identifying the risk is very important for the execution of the next stages of the risk management process. If we don't identify a risk in this stage this means that

will not be included in the further analysis (ISO, 2008). Further, this process an ongoing effort to check the environment for emerging and changing risk conditions to regularly review and refocus for dealing with threats (Hill 2000).

Various techniques are applied for finding all the potential risks which might impact the organization, such as checklists or breakdowns, risk workshops, examination of corporate processes, internal inspections and interviews, loss balance and recommendations by external experts, scenario analysis or risk mapping (Rosman, 2009).

2.2.2. Risk Assessment – Risk Analysis

The second stage of Risk Management process is where collected data about the potential risk are analyzed. Risk assessment is defined as the evaluation and estimation of the levels of risks involved in a situation, their comparison against benchmarks and determination of an acceptable level (ISF, 2010). Risk assessment follows the risk identification and its purpose is to evaluate how big the risks are, pay attention to the most important threats and opportunities, to measuring and prioritizing risk (COSO, 2004).

According to McCuaig (2008) Risk assessment should answer the following five questions:

- What can go wrong?
- How can it go wrong?
- What is the potential harm?
- What can be done about it?
- How can we stop it from happening again?

Risk assessment process contains different activities, the first activity is to develop a set of assessment criteria between the business units. Assessing can be accomplished in two stages. In the first stage an initial check of the risks is taking place using qualitative techniques and the second stage where the most important risks are assess using qualitative techniques. It is very important for a company to manage the risk interactions. Insignificant single risks can create

significant problems in an organization if they interact with other events and conditions. Consequently, companies are using a holistic analysis of risks by using techniques such as risk interaction matrices, bow-tie diagrams, and aggregated probability distributions (COSO, 2004).

Risk assessment in an organization should have a form of measurement of risk where there will be a standard of comparison to compare and aggregate risks across the organization. A method that most organizations using is the scales for rating risks in terms of impact, likelihood, and other dimensions. The more descriptive the scales are, the users will be able to have better interpretation of the risk (COSO, 2004).

According to Lichtenstein (1996) the selection of the most appropriate methods in risk assessment can be influenced from different factors in order to find the best fit for the right purpose. Each organization should decide which of these factors are the most serious for them and develop the assessment accordingly. In a survey conducted by Lichtenstein (1996), many factors were discovered, but the most important ones are:

- Adaptability, the need of adapting to the organization's requirement
- Cost of using the method, both the employment cost and the method itself
- Completeness, the method needs to be achievable
- Complexity, how limited and simple the method is
- Validity, the results should be valid
- Usability, the method should be understandable to use
- Credibility

2.2.3. Risk Control

Risk control is the third stage of Risk Management Process many activities take place to prevent losses or reduces their severity (Valsamakis et al., 2000, Williams et al., 1998). Risk control is defined by Valsamakis et al. (2000) as a method of countering risk at the source of the risk. Further, Young (2006) defined the risk control as the application of techniques to reduce the probability

of loss which has as goal to minimize the potential effect of the identified risk and it aims to eliminate or minimize the potential effect when an identified risk occurs.

The main risk control activities objectives are:

- To minimize or reduce the risk factors giving rise to a loss.
- To decrease the actual loss if preventative controls were not fully effective.
- To avoid potential catastrophic events.
- To enhance the understanding of risks throughout all organizational levels.

The Risk Control activities should consider the likelihood of loss occurrence and how important are those loses for the organization (Valsamakis et al., 2000, Young, 2006). A risk Control programs includes all the risk control activities, the analysis of all risk factors like the cause of losses, the action plans and procedures (Young, 2006). When an organization is designing, implementing, evaluating and improving risk controls, should have in mind the characteristics of good controls too, such as (Young, 2006):

- Controls should be logical, focused and provable.
- Controls should be timely and accurate.
- Controls should be reviewed and adjusted when deficiencies are identified.
- Controls should be improved continuously due to changing conditions.

There are three types of risk controls that helps to minimize organizational risks:

- Preventative controls: These controls are designed and applied to proactively avoid loss events from happening.
- Detective controls: These controls recognize loss events as soon as they occur, to boundary the effect of the occurrence on the organization.
- Contingency controls: These controls guarantee the sustainability of an organization once a risk event has occurred.

Risk control activities emphasizes to the disadvantages of a risk, to prevent the negative consequences of a risk event (Young, 2006).

2.2.4. Risk Monitoring

Risk monitoring is the final step of risk management process, is a vital because all the information gathered from identifying risks is collected and monitored (Winch, 2002).

Within Risk monitoring an organization can ensured the effectiveness of its risk management techniques and activities based on organization's policies and procedures (Hollman & Forrest, 1991:63; and Young, 2006:34). In risk monitoring activities can be found that existing controls are inefficient and the must be revised or to implement new controls, thereby improving the organization activities (DEAT, 2006).

Continuous monitoring is very important for an organization, since the environment changing constantly, new developments and the potential impact of these on the organizations risk exposure. The monitoring must be executed by internal and external audit, investigations, and reporting. Those activities should contain clear and relevant information about the risk control actions taken, the preparedness of the organization to deal with risks (Kubitscheck, 2000, Bowden et al., 2001, Andersen & Terp, 2006). During Risk Monitoring tools and techniques used such as (PMI, 2004):

- Risk reassessment – identification of new potential risks.
- Monitoring of the overall project status – are there any changes in the project that can affect and cause new possible risks?
- Status meetings – discussions with risks owner, share experience and helping to manage the risks.
- Risk register updates

2.3. Risk Management in Banking Sector

Risk Management is very important procedure for the operation of a bank. Every risk manager is gathering different information and is using different methods and these depends on the degree of bank development. Further, these is happening because of the different type of banking risks (For Example: credit, market, operational) that a bank must encountered, as a result a risk manager needs to require specific data for their evaluation and also, risk management information depends on the banking system (Poliakov, 2011).

Banks are dealing every day with different types of risks, operational risk, financial risk, and this is resulting that risk management to play a significant role in their operations (Carey, 2001). Hence, banking institutions since they cannot eliminate the risks, should have as priority the risk management, should also have an internal control system for decrease the level of exposure to risks that banks face, and the possible negative costs of any risk (Carey, 2001). The banking risk management deals with controlling the risks. According to Ismal (2010) the banking risks are correlated, this means that the consequence of one risk has effects on the other. Moreover, Santomero (2003) stated that the correlation of different bank risks may have balancing effects on each other. Most of the Multinational companies have embedded the risk management process to their business (Hagelin and Pramborg, 2004).

Managers satisfy their needs of risk taking through the Risk Management process (Ozturk, 2007). The realization of this need is achieved through the key risks identification, the analysis and assessment of this risks, by selecting which risk should be increase and which should be reduce and how to face it. Furthermore, managers must set up a procedure for monitoring those risks. In addition to this, managers should also establish a risk assessment process for measuring the risk and mitigating the exposures so that the bank objectives are not affected (Awojobi.et al, 2011). Risk management in banking sector is influenced from the employee's perception, in particular, the risk assessment and the decision maker is performed by the bank's employees as a result their decisions are more concerned with their own biases, and not the organization's

goals when conducting risk assessments (Carroll, 1998). Carroll (1998) found in his research that in case of loans, bank employees tend to imitate the risks associated with lending to new customers and overestimate the risks associated with lending to their existing customers. This happens because of the bonuses they received for getting new customers (Carroll, 1998).

One of the main goals of the banking risk management is to avoid the insolvency situation. The efficiency of banking risk management is used to indicate the solvency level. According to Saunders and Cornett (2006) one of the features of insolvency is the capital degradation and liquidity issues. The Liquidity issues happens when the bank bankrupt, which means that the bank is unable to meet the short-term obligations and is compelled to liquidate part of its assets. In a period of capital degradation bank should close its business as its liability becomes greater than its assets (Awojobi.et al, 2011). Most of the bank's managers, emphasizes on profitability by fulfilling the short -terms objectives and in the process, they do not consider the risk management process (Aremu et al., 2010).

In the 1950s Harry Markowitz developed a modern portfolio theory, on financial risk management in his paper “Portfolio Selection” (1952) but a lot of things has change in the banking industry from then. In 1997 Pyle stated that risk management process among banks was inadequate and should create a uniform procedure to monitor and analysis of risks. In 1988, Basel committee proposed Basel I for capital accord on banking supervision. The aim of Basel I to introduce an international standard that could be applied by the regulators, when formulating regulations regarding a bank’s requirement of capital. One of the key information of Basel guide was related to capital adequacy which banks must use as a mitigating mechanism when a bank’s assets are exposed to risk. When a financial institution receives higher exposure to operation and credit risk, there will be a need for its capital to supplement itself to make sure that future operations are safeguarded in case that the risk leads to losses (Awojobi.et al,2011). Following that, in 2004, Basel II was proposed, which is focused on the limit of the capital that a bank must hold (Calem & Rob, 1999). Basel Committee

on Banking Supervision developed a new international regulations guide Basel III, which includes strict capital rules which will force all banks to increase more than three times the capital amount to avoid the future rescue by taxpayers. Basel III has as goal to improve the quality of risk management in the banking business, which will have as a result enhance financial system stability (Moshinsky, 2012).

Nowadays, all global and international organizations relating with banking institutions like Bank for International Settlements, the Basel Committee on Banking Supervision, are paying more attention to resolving the issues of financial risk management and control. For example, Basel Committee developed the Core Principles for Effective Banking Supervision, which is about the need for the banks information systems to allow to accurately assessment, monitor and adequately control the financial risks (Basel, 2011).

Risk management is very important to the banking industry. The banks provide us very important services like lending, borrowing and accounts that facilitates payments for our development (Sveriges Risk bank, 2011). People, Business depend on the banking sector, therefore, the procedures and regulations for risk management in banking should constantly updated. These regulations are mostly set by the Basel committee in the form of Basel 1, 2 and 3 (BCBS, 1988; 2004; 2010).

2.3.1. Types of Risks in Banking Sector

Every sector must face different types of risks. Risks connected with the banking services depends on the type and the natures of the service provided. The number of risks that a bank is dealing with are associated with the changes taking place in economic, social and political environment. Machiraju (2008) stated that banks must manage four significant types of risk to earn profits for increasing shareholders wealth. These are credit risk, interest rate risk, liquidity risk, and operational risk.

Banks are dealing with different risk, these risks can be divided in two different categories, business risks and control risks. Business risk are the risks connected with the bank's operations. These risks are capital, credit, market, earnings, liquidity, business strategy and environmental, operational and group risks. On the other hand, control risks measure the risks appeared from lapses in internal controls, management, organizational structure and compliances (Arora, 2009).

In Basel Capital Accord are mentioned three main categories of risks, Credit Risk, Market Risk and Operational Risk (Basel, 2003).

Credit Risk: is defined as the risk where the possibility of losses is associated with the failing of customers to comply with their obligations to their loans (Basel, 2003).

Market risk is the risk arise because of the changes in the market variables. Market risk management, measures, monitors, manages liquidity, interest rate, foreign exchange and price risk (Basel, 2003).

Operational Risk. According to Basel Committee on Banking Supervision (2003) operational risk can be defined as the risk which is connected with the failure of the internal procedures, people, systems, external events.

2.3.2. Risk Management in Bank: Basel Committee Approach

The oldest international financial institutions with headquarters in Basel, Switzerland, is The Bank of International Settlements (BIS). Bank of International Settlements acts as central bank and the main tasks is to serve central banks and promote international co-operation (BIS, 2012). The Basel Committee on Banking Supervision (BCBS) secretariat is located at the Bank of International Settlements and involve of representatives of many (BIS, 2012).

Basel Committee goal is to improve the understanding of some key supervisory issues and to increase the quality, worldwide, of supervision of banks (BIS, 2012b). The Basel Committee have published three main agreements, Basel 1 (1988), Basel 2 (2004) and Basel 3 (2010), the same time, minor modifications

were made to obsolete agreements before a new agreement was reached (BIS, 2012, BIS, 2012). A new agreement was drafted when the previous one is outdated by changes in the banking environment, for example the global financial crisis in 2008-2009 led to the creation of the Basel 3 agreements (BCBS, 2010). The Basel Accords are only recommendations, since the Committee has no official supranational authority (BIS, 2012). It is rather the member states that must adopt the suitable approval procedures in their respective countries to make the references appropriate by law (BCBS, 2004). The EU applied the first two Basle agreements and Basel 2 was applied as a law in the EU Member States in 2007 (Holmquist, 2007).

Historically, in 1988 the Banks of International Settlement (BIS) decided to establish Basel Committee on banking supervision and issued guidelines for updating risk management in banks. The purpose of this Committee is to help the banks to identify the various types of risk and to take appropriate measures to overcome the capitalization of bank assets and to reduce the credit and operating risks faced by banks. The Basel Committee guidelines create a standardization and universalization between the banks in the part of risk management and pursue to protect the interest of the depositors/shareholders of the bank.

Under the published guidelines, capital adequacy was considered a panacea for risk management and all banks were required to have a Capital Adequacy Ratio (CAR) of at least 8%. CAR is the ratio of risk-weighted assets and provides margin to depositors in the event of bankruptcy. In January 1999, the Basel Committee proposed a new capital pact, known as Basel II. A framework for measuring and quantifying the risk associated with its banking operations. The emphasis of the New Basel Accord is based on flexibility, efficient operation and higher revenue for banks with full risk recognition. The new guideline makes a clear distinction between credit risk, market risk and operational risk that provides for the risk weighting covering all three categories separately. Furthermore, Basel II Accord specifies various options for clarifying the capital requirements for credit risk and operational risk. All global banks should select

methods that are most applicable for their operations and financial markets. In June of 2004 the Basel II Accord was published. The finalized Basel II Accord is based on three pillars: Pillar I: Minimum Capital Requirement, Pillar II: Supervisory Review, Pillar III: Market Discipline.

Minimum Capital Requirement (Pillar I) is determined by the capital ratio which is defined as (Total Capital - Tier I + Tier II + Tier III) / credit risk + market risk + operational risk). In the first Basel quid line (Basel I) provided only a credit risk. In 1996, market risk was added. In the first stage, all banks should follow the standardized approach to credit risk, the approach of key indicators to operational risk and the standardized approach to market risk. The transition to higher approaches will require an RBI license. After the sound risk management, the use of higher approaches, which are more risk-sensitive, can contribute to reduce capital requirements for banks.

Supervisory Review Process (Pillar II) is obligated to provide to Risk Management process with adequacy and integrity. There are four key rules of supervisory review, according the Basel Committee:

- The bank should have a process of access to its overall capital adequacy in relation to its risk profile and a strategy to maintain its capital levels.
- Supervisors expect banks to operate above the minimum capital adequacy ratios and to ensure that banks hold funds that are above the minimum.
- The supervisory authority examines the bank's assessment, internal capital adequacy and strategy, as well as compliance with capital adequacy ratios.
- Supervisors should pursue to intervene at an early stage to prevent the downgrading of funds below prudent levels.

Market Discipline (Pillar III). To have Effective market discipline, banks need to have reliable and timely information, which will allow to all parties to carry out an established risk assessment. Pillar III refers to periodic disclosures to the regulator, the board and the market regarding various parameters that indicate the bank's risk profile. Following these guidelines, ensures security and

robustness in banks and the financial system and makes it easier for banks to carry out their activities in a safe, healthy and efficient way.

Basel Committee on Banking Supervision developed some new international regulations which has as main purpose to decrease the possibility of a next large-scale financial crisis. Basel III includes strict capital rules that has as a result, for banks, to increase more than three times the capital amount to avoid the future rescue by taxpayers. Moreover, with the new Basel III, banks should be able to improve the quality of risk management and provides stability to the banking system.

2.3.3. Basel II and the effects on banking sector

Basel II agreement was issued to replace the first Basel, in an updated and improved version (Das, 2007). A main part of this development was the banks to fulfil with various qualification requirements meant at reducing operational and governance levels. These improvements have exceeded the traditional method of filling compliance and creating an increased risk reduction culture, combined with the use of a variety of models and the creation of high levels of transparency. In this context, the banking supervisors were given a lot of responsibility, who were informed to ensure that the underlying assets were properly committed, while at the same time providing incentives and consequences aimed at safeguarding good risk management practices (McLaughin, 2008). Furthermore, Basel II established the need for banks to be more effective in monitoring and updating banks' risk assessments on specific borrowers to ensure ongoing risk assessment and management (Paletta, 2004).

According to Wellink (2008) Basel II was a step forward for banking regulations and will help the banks to be more prepared for the challenges of the market. This banking regulation provide instructions for all the type of risks that a bank will face, contribute sound risk management practices and helps the general level of market discipline. Chatterjee's (2007) stated that one of the disadvantages of Basel II is that different banks will use different models to assess their risk profiles (Chatterjee, 2007).

In addition, there have been serious criticisms of the capital rules governing Basel II.) Capital adequacy rules will tend to aggravate market cycles, therefore encouraging economic growth and failure ((Fournier et al, 2008). This is since in a rising market, profits will quickly improvement regulatory capital that encourages significant additional loans, while in a fall in market assets, the decline in assets will reduce regulatory capital by creating a decrease credit cycle. Therefore, Fournier et al (2008) said that the Basel Committee should also execute influence ratios to support risk capital requirements that are more risk-sensitive to create fully effective arrangements. Another serious criticism is that Basel II has created significant incentives for banks to migrate risk to unregulated institutions such as hedge funds. This helped the liquidity crisis with the credit crisis, giving the hedge fund much more funds with much higher moral hazard levels (Wood, 2007). Wood (2007) also stated that the deal has been criticized as it has led banks to make great efforts to remain compatible and, consequently, to divert banks from real risk management practices.

The implementation of Basel II to the banks process created major problems because of the structure of the approach (Herring, 2007). The agreement has failed to address the competitive imbalances that exist in many developed banking markets. This has as a result, lower and more variable capital costs than initially expected for many banks. Some banks stated that they prefer more simple and standardized approach, while others have followed the approach of advanced internal ratings, which has as outcome the agreement to be weakness and not effective. This led to the argument that an equal or greater improvement in risk management could be achieved, while reducing compliance costs and reducing the uncertainty about the influence on total financial constancy (Herring, 2007). Therefore, the Basel Committee on Banking Supervision has identified and examined the issues of this guideline and it published a paper on additional risk burdens (Sawyer, 2009).

2.3.4. Risk Management and Value Creation in Banks

Value-to-risk analysis refers to any risk management and valuation analysis, it is a risk-quantifying tool which first was used in trading risks (Leong, 1996). Value

to risk analysis has been used to assess the levels of interest rate risk and credit risk. In the case of the banking industry, value-at-risk represents a more difficult way of examining the volatility of the bank's equity. Nevertheless, such an approach is not always helpful for the bank. This is since value-at-risk measures on stress tests, include imitations where several assumptions are required. Therefore, there is no standardized way to accomplished risk analysis (Leong, 1996). This means that, the bank is required to depend on on assumptions that may not be valid, and these hypotheses may be a source of risk.

The value-at-risk measures are based on three different approaches, each method producing different results of value-at-risk measurement with different advantages and disadvantages. By comparing the actual variability of the sources of risk with the historical sensitivity of these sources, the result is the historical value at risk and provides an adequate assessment of the future. On the other hand, analytical risk is based on the analysis of the variables that can affect the value and risk of a service, such as interest rates, default risk and exchange rates. Although this method is easy to perform, it is very vulnerable to the validity of assumptions and does not always accurately judge the risk of unlikely events. Finally, the Monte Carlo approach offers the greatest precision, by creating scenarios which include all the potential risks and changes in value and determining what is the most likely value-at-risk for these scenarios. While this approach is best for collecting factors such as the risk of choice, it is very time-consuming (Lang and Nayda, 2008).

Basel Committee on Banking Supervision has included a regulatory capital charge for operational risk and value-at-risk which was very important for the value - at -risk concept. Ebnöther (2003) stated that the level of operational risk can be easily measured for a single bank unit, because work flows are defined, but this is not necessarily the case for the bank. A small percentage of all bank business flows make a significant contribution to the overall value that runs the risk of the bank. To determine the correct capital charge to be applied and to distinguish the different characteristics of quality management and risk

management respectively, it is important to analyze the value-at-risk and the effective calculation and test durability stress testing (Ebnöther, 2003).

On the other hand, value at risk even if it's a useful tool, will never fully describe the overall size of a bank's exposure to risk (Economist, 2004). Hence, value at risk is a good measure to define the risk under normal conditions and not in unexpected condition. When the risks cause significant market shifts, making banks' estimates of the diversity and stability of their portfolios inaccurate, by adopting value at risk measure is almost useless (Economist, 2004).

2.4. Operational Risk Management

Historically, Operational risks was appeared in the insurance, and are usually hazard risks. Despite that, now, the operational risk has more specific definition and it has evolved as a term, especially in the financial sector. In the financial institutions, the operational risk is differentiated from the other risks because you measure this risk in terms of potential economic losses (Hopkin, 2010). It is very important to managing operational risk to all business environments. Operational risk has been defined as the risk that will interrupt normal everyday activities. According to the FIRM risk scorecard classification system, operational risk is similar with infrastructure risks (Hopkin, 2010).

At first the operational risk, was difficult to be identified and measure with the traditional ways (Power, 2005). The past years, researchers take an interest to the phenomenon of operational risk and they developed standards and frameworks. Operational risk was defined as the risk of loss because of the insufficient or the failure of the people, internal processes, systems and external events (BCBS, 2006).

Operational risk management has developed its own management structure, tools and processes. In the past, it was difficult to quantify, manage in traditional ways and insure the operational risk, it was an incomplete category. Until the late 1990s there weren't a lot of researches concentrate to Operational risk.

One of the very first studies for Operational risk management were published by Embrechts et al. (1997) who did the modelling of extreme events for insurance and finance. Moreover, Embrechts after his first study in 1997 he conducted further research in the concept of operational risk Embrechts et al., 2003, Embrechts et al., 2005 and Embrechts et al., 2006)and his work has become classic in the operational risk literature.

Besides, Embrechts, some other researches did other early studies on operational risk management, Cruz et al. (1998), Coleman and Cruz (1999) and King (2001). Then, researches focused their studies in operational loss data (Van den Brink, 2002, Hiwatshi and Ashida, 2002, de Fontnouvelle et al., 2003, Moscadelli, 2004, de Fontnouvelle et al.2005, Nešlehová, 2006, Dutta and Perry, 2007). Moscadelli (2004), performed the most important operational risk research. More specific he performed a detailed Extreme Value Theory (EVT) analysis of more than 47,000 operational losses.

The risk managers' use the Operational risk modelling helps in order to have better treatment of the operational risk and efficient risk manage. In the studies of operational risk, researchers developed a lot of techniques and methodological tools and models for operational risk management such as Extreme Value Theory (Cruz, 2002, Embrechts et al. ,2005, Chernobai et al., 2007), Bayesian inference (Schevchenko and Wuthrich, 2006, Cruz, 2002), Dynamic Bayesian networks (Ramamurthy et al., 2005) and Expectation maximization algorithms (Bee, 2006).

During the years, were established many definitions of operational risk. Jorion (2000) said that the operational risk is a risk associated with human and technical errors and accidents. According to King (2001) operational risk is a measure connected with an organization business activities and the difference in its business. Furthermore, CIMA Official Terminology (2005) stated "Business operational risk relates to activities carried out within an entity, arising from structure, systems, people, products or processes.' Basel Committee (2004)

defined the operational risk as the risk of loss because of the insufficient or failure of the internal processes, systems, external events or people.

Operational risk management is associated with organization's risk appetite. The factors such as the size and the type of organization, its capacity of risk and its ability to exploit the opportunities and to withstand the difficulties, influence the risk appetite. Once determined the severity of the risk then the risk should be controlled by using one or more of the following methods:

- Accepting the risk
- Sharing or transferring the risk
- Risk reduction
- Risk avoidance.

Operational risks are difficult to measure or manage before the risk occurs and is not possible to determine the impact of the risk. The harshness of the risk may be underestimated. The continuously changing of the business environment is one of the issues with operational. According to the Turnbull Report (1999), which is a guidance for directors on the Combined Code:

'A company's objectives, its internal organization and the environment in which it operates, are continually evolving and, as a result, the risks it faces are continually changing. A sound system of internal control therefore depends on a thorough and regular evaluation of the risks to which it is exposed.'

During the operational risk management should have established also the process of monitoring the risk and reviewing and reporting on a regular basis. Therefore, loses related to operations can arise at all levels of organization, from board of directors till groups of people (Jongh et. al., 2013). Furthermore, loss from external risks (e.g. natural disaster and terrorism) are easier to identify than loss from internal events (e.g. employee fraud and system failure), as a result the internal operational risks are usually closely connected to the activity of a particular organization. During the adopting of changes, the reports and reviews for the operational loss should be detailed and cover all the

comprehensive and clear classification of all internal weaknesses (Apatachioae, 2014).

2.4.1. Identification of Operational Risk

Operational risks are often invisible than other risks and it's difficult to identified it from the beginning. There is a variety of range of the operational risk, a very small like the risk of loss due to a small human mistake, and the very large, for example the risk of bankruptcy due to serious fraud. Operational risk can happen at every level in an organization (CIMA, 2008).

There are different types operational risk related to business (CIMA, 2008):

- Business interruption
- Errors or lapses by employees
- Product failure
- Health and safety
- Failure of IT systems
- Fraud
- Loss of key people
- Litigation
- Loss of suppliers.

The practices that are related with controlling the Operational risks within an organization are risk assessment and risk management, including internal control and insurance. The external and internal environment of an organization are the resources for Operational risk and are caused from people, processes and technology. One of the most essential parts of managing risk is Identification process. If an organization failed to identify a risk this will gave as result that no action is taken to manage that risk (CIMA, 2008).

Furthermore, an organization can use different techniques to identify risk. One of the most use method for identifying a risk is the use of workshops to 'brainstorm'. "Brainstorm" method can be used at different levels of the organization and can, very quickly, to identify a large number of risks. In this

method is very important to stay focus on identifying the risks and not to move one to the next step of evaluating the risk (CIMA, 2008).

Moreover, the technique of audit can be used to identifying operational risks since operational risks are mostly based on procedures and processes. Besides that, audit can be used as a method of reporting to the organization board about the effectiveness of risk management framework. (CIMA, 2008).

Additionally, another tool for identifying operational risk is by finding critical dependences in people, processes, systems and external structures, once identified, the dependencies can be. Physical inspection and incident investigation are approaches used to identifying operational risks too. After the identification and categorization of the risks, it is possible for the organization to proceed with the assessment and management of the risk (CIMA, 2008).

2.4.2. Definition of Operational Risk Factor

The risk factors that operational risk deals, are the factors that create losses that can negatively influence profits (King, 2001). According to Katz (1995) every organization should make an early assessment of the underlying risk factors that relate to it. When the risk factors are being identified then the operating, credit, accounting reporting and risk management processes will be put in place.

During the risk allocation process assessment take place to measure of the extent to which a risk factor increases or decreases the expected volatility of earnings (Davies et al, 1998). Generally, for monitor and control the risk effectively, the sufficient identification of the risk factors is a vital process for an organization.

The definition of operational risk, identifies four risk factors, people, processes, systems and external events. These factors apply to an organization's business environment and control, although in terms of operational risk management, the following risk factors could determine the level of operational risk:

- Type of business activity
- The size of the activity;

- The business environment
- The control environment (Ong, 2007).

Furthermore, it is very important that the recognized factors must be quantifiable to confirm that they can determine the level of risk. Ong (2007) said that defining the degree of risk is an important point, which should provide details of the level of the risk factor and what should be done about it. Hence is obligatory to link a value to risk factors in order to determine the level of risk. Thus, the risk factor as well as the level of risk must be clearly identified in the management of key risk factors.

2.4.2.1. People

According to Katz (1995), in any business activity there is always a human factor that should be considered. People's knowledge, capability, reliability and experience are critical risk factors of the business process.

People risk was defined by Hoffman (1998) as the risk of intentionally or unintentionally loss by an employee or involving an employee. Donahoe (1999) stated that people risk includes ineffectiveness and fraud.

For any organization, the most important resource are the people within the organization (Kingsley et al, 1998). People risk factor includes:

- Human error
- Lack of integrity and honesty
- Lack of separation of duties
- Lack of customer focus and professionalism, lack of teamwork and respect for the individual
- Dependence on key individuals
- Insufficient skills, training, management or supervision
- Lack of culture control

The people risk factor is a major contributing factor, which has several difficulties to measuring it but has as a result huge failures for an organization, therefore, it should be included in any process that aims to improve risk management (Kingsley et al, 1998).

During the operational risk management process, can be identified a sub –risks of people as risk factor. Rachlin (1998), identified the following sub – risks:

- Integrity: which includes the fraud, collusion, malice – unauthorized use of information, rogue trading
- Competency
- Management
- Personnel
- Health and Safety

According the Financial Services Authority (1999) there are key sources of people risk:

- Inexperienced, useless, inappropriate, negligent and maverick staff
- Human error
- Working culture creating low morale, high staff turnover, poor connection, low productivity and industrial action
- Fraud and theft
- Unauthorized and poorly informed decision making at all levels, specifically with connection to business strategy, project management, change management, liquidity and outsourcing

Furthermore, Katz (1995), identified the below employee risk factors:

- Fraud
- Malicious neglect
- Neglect of duties
- Lack of knowledge

- Lack of motivation

People risk factor is not only responsibility of the human resources department even though they do help to controlling of the risk (Wilson, 2000). Every business department have their own responsibilities on the control of the operational risk (Wilson, 2000).

2.4.2.2. Systems (Technology)

The failure of applications systems for meeting user necessities and the absence of built-in control measures consist the System risk factor (Hopkin, 2010). System failures are included on Operational risk definition and those failures could happen from various factors. Basel (1998) stated that by choosing systems that are not well designed or implement then bank is dealing with risk, further the rapid technological changes can create more operational problems with new or updated systems (Basel,2008). The new technologies have consequences of complexity and uncertainty, as a result a greater risk. Remenyi and Heafield (1996) argued that new systems might need adjustments to work as expected. With the development of technologies, new skills required from employees. Some of the employees might be resistance to the learning new technologies. Hence, this resistance should be monitored and controlled and at the same time effective training programs must be applied.

Basel Committee (1998) listed possible risks related to systems failure:

- Counterfeit electronic money
- Risky Service provider
- Uselessness of systems could cause delays or disruptions

According to Wilson (2000), the definition of system risks includes external pressure, for example the risk of not follow the technology development. Furthermore, Wilson (2000) stated that technology risk can be appeared from the contracts for maintenance on existing information technology infrastructure and application software, or outsourcing the IT services or projects. Wilson

(2000) also argued that should be an assessment of the technologies from the operational risk manager, by examining an organization's compliance with technology controls. Those controls can protect the organization from data stealing, voice equipment failure, human errors and minimize any other exposure.

2.4.2.3. Processes

Operational risk definition besides the people, and the systems includes also the processes. Process risk can be defined as the risk of the business processing which is insufficient and causes unexpected loses (Wilson, 2000). In order, an operational management of process risk to be proactive should include prompt, accurate and effective data collecting and processing (Kingsley et al, 1998). Additional, process risk contains execution errors, which operational risk management should also identify this error and prevent them from happening. If this execution errors occur then operational risk management must minimize their effects on the organization (Crouhy et al, 1998).

The quality of data integrity is being control from the process environment and this includes the static data, for example the data concerning customers and instruments, and transaction data, for example data which is about trades and positions (Davies et al, 1998). The process risk can be found in any step of the business environment hence it should identify where the risks are within each environment. Davies et al (1998) stated that the determination of the risk can be done by looking at the process flow of a single trade and control where the risk occurs and how it can be measured. In conclusion, the sub –risk factors of the process are the processing of new products, recording and reporting, business process, settlements and controls.

2.4.2. 4. External Factors

External Factors have an impact and control of the organization, and have an adverse effect on the internal operational factors, people – processes – systems. In 1999 Price Water House Coopers conducted a research which was about the external events relating to operational risk and include:

- Systemic risk
- Exposure to other industry participants
- Physical and natural disasters
- A change in law, regulation, tax, accounting

Moreover, Financial Services Authority (1999) stated that fraud risk is an external risk factor. Fraud risk is the risk from the illegal actions of an employee, customer, and involved different parties to a transaction or outside intruders (Mayland, 1993). According to Rachlin (1998) there are sub factors of external risk which are:

- Outsourcing, external supplier risk
- Physical security
- Money Laundering
- Compliance
- Financial Reporting
- Tax
- Legal
- Terrorist threat
- Natural disaster
- Strike risk

2.4.3. Evaluation of Operational Risk: Qualitative & Quantitative

According to Cagan (2001), Cumming and Hirtle (2001) and Khan and Ahmed (2001) there is a differentiation between the operational risk measurement and operational risk management. Risk measurement process is to quantify the risk exposures, on the other hand, risk management is an overall process for defining a business strategy, identify the risks to which it is exposed, to quantify those risks, and to understand and control the nature of risks an organization faced.

The aim of Operational risk measurement is to calculate the capital for operational risk. Basel II (2006), delivers three methods for calculating operational risk capital:

- The Basic Indicator Approach
- The Standardized Approach and
- Advanced Measurement Approaches (AMA).

The Basic Indicator Approach (BIA) must have an operational risk capital equal to the average of the previous three years of a fixed percentage of positive annual gross income. Data for each year in which gross annual gross income, when it is negative or zero, should be excluded from the numerator and denominator when calculating the average. The Basel Committee proposes gross income as the only exposure indicator. The definition of Gross income is the net interest income plus net interest income.

According to of Basel Capital Accord (2006) in the Standardized Approach (TSA) the activities of the banks are divided into eight business lines: corporate finance, trading and sales, retail banking, commercial banking, payment and settlement, agency services, asset management and the stock market. In each business line, gross income is an extensive indicator that serves as a substitute for the scale of business activities and therefore for the potential scale of exposure to operational risk in each of these business lines. The capital charge for each business line is calculated by multiplying gross income by a factor (declared beta) that corresponds to that business line. Beta serves as a substitute for the relationship between loss of operational risk for a given business line and total gross income for that business line. Further, in the standardized approach, gross income is calculated for each business line and not for the whole institution.

Last, Advanced measurement approaches (AMA) based on Basel II (2006) is the regulatory capital requirement will be equal to the risk measure generated by the bank's internal operational risk measurement system using the quantitative and qualitative criteria for the AMA. In addition, the suitability of the allocation methodology will be reviewed considering the stage of development of risk-sensitive allocation techniques and the extent to which it reflects the level of operational risk in legal entities and the banking group. Supervisors expect that

AMA Banking will continue their efforts to develop more and more risk-sensitive operational risk allocation techniques despite the initial adoption of gross-income-based techniques or other attorneys for operational risk.

2.4.4. Control of Operational Risk

Risk Control is a process for preventing losses, minimizing the results of loses from the risks that an organization is dealing with. Risk control activities can be categorizing as follows (Vaslamakis et al, 2000):

- Activities focused to control the possible adverse incidence of an event and then attempting to eliminate it and
- Activities aimed to minimizing the loss after it happened
- Kingsley et al. (1998) listed some objectives of the control of Operational Risk:
- Avoid potential catastrophic losses
- Generate a wider understanding of operational risk issues in all organization process
- Allow the organization to be dealing with risks more effectively
- Provide objective measurement of performance
- Change behavior to decrease operational risk and improve the culture of control within organization
- Provide objective information in order the services offered by the organization takes account of operational risks
- Provide support to ensure that due diligence is given when conducting mergers and acquisitions

2.4.4.1. Operational Risk Policy

Operational risk management policy is the concept used to communicate to all involved people in an organization, the company's approach on the operational risk management. Policies contain the definition of operational risk, the organizational approach, the roles and responsibilities, the key values for management and information and technology (Financial Management

Accounting Committee, 1999). Furthermore, an operational risk management policy should also include:

- The management principles for operational risk: company's philosophy and principles on operational risk
- Definition and classification for operational risk
- Objectives and goals
- Operational risk processes and tools: such as risk assessment, measurement, reporting, and management processes
- Organizational structure
- Roles and responsibilities should be defined for every key aspect of operational risk management

Freeman (1999) argued that organizational structure it will be nonfunctional if there isn't a suitable policies and standards and controls. Moreover, Risk Management policy must identify the internal controls that are important to monitor the organization's risks (Carr and Walsh, 1999).

2.4.4.2. Internal Controls

Internal control is an important feature of operational risk management and provides rational assurance that the organization's objectives are being met. The combination of an effective risk management, reliability of financial reporting (COSO, 2013), compliance with applicable laws and regulations, the execution of internal control system can be achieved. Internal Controls are separated into two categories, the primary and secondary controls. Primary controls prevent a mistake from happening and secondary controls is identifying potential results (Schwartz and Smith, 1997).

Additionally, Chernobai, Jorion & Yu (2011) stated that weak internal controls were as result, most of the times, operational risks. The most common internal control frameworks, that banks used, is the monitoring and reporting regulations, and risk governance. According to KPMG (1999) the main principles of internal controls includes:

- Management supervision and the control of culture
- Risk Assessment
- Control Activities
- Information and Communication
- Monitoring Activities
- Evaluating of internal control systems by supervisors

Risk control is an ongoing process, it makes sure that risks are continually reevaluated and all the business aspects are complied with the policies and procedures (KPMG, 1999).

2.4.4.3. Risk Reporting

Risk policies and internal control together with risk reporting plays a vital role in risk management process. The risk reporting is the process where an organization reports their risks to its shareholders and regulators (Goldman et al, 1998). Effective risk reporting framework includes all the risk management information that meets the objectives of an organization and needs the coordination of the board of directors and managers.

Further, Howell (2014) stated that effective risk reporting can be accomplished if there is a close collaboration between board of directors and senior management where management will provide information and will explains the key performance indicators. Also, switching from traditional reporting to digital technologies allows more quality information to be distributed and gives more time for analysis, which in turn increases the quality of the reporting (Howell, 2014).

2.4.5. Operational Risk Management in the banking sector

In financial Industry, the most discussed topics is the Operational. This attention to operational risk in the financial industry can be attributed to higher investment in information systems and technologies, the growing wave of mergers and acquisitions, the emergence of new financial instruments and the development of e-commerce (Sironi and Resti, 2007).

The most commonly used definition of Operational Risk which fits to all banks is the one of Basel Committee "The risk of direct or indirect loss resulted from inadequate or failed internal processes, people, and systems or from external events" (Basel, 2001a, para 6).

According to Basel Committee on Banking Supervisions (2006) definition, there are four causes of operational risk, process, people, and system or external events.

The PNC Financial Services Group (2001) stated that the operational risk definition should include the direct losses from the internal events, illegal behavior, errors on systems and processes or external events and exclude the business, strategic and reputational risks.

According to Lam (2003) Operational risk management contains many activities such as:

- Developing policies and internal standards
- Developing key risk indicators
- Planning management of major business disruptions and
- Keeping a database of operational risk incidents.

Since the end of 1980s, Financial institutions have faced more than 100 operational loss events exceeding $100 million (De Fontouvelle et al., 2003). The highest losses from operational risk have been recorded in Societe Generalé in 2008 ($7.3 billion), Sumitomo Corporation in 1996 ($2.9 billion), Orange County in 1994 ($1.7 billion), Daiwa Bank in 1995 ($1.1 billion), Barings Bank in 1995 ($1 billion) and Allied Irish Bank in 2002 ($700 million).

In addition, in Central Europe there have also been several cases of operational risk. For example, in 2000 a trader and his manager in one of the largest Czech banks exceeded their trading limits on the sale of US government bonds and caused losses of $ 53 million to the bank. At the end of the 1990s another Central European bank suffered a loss of $ 180 million as a result of providing funding to

a company based on fake documents. Other general operational risks in central European banks, such as cash theft, rounding errors in computer systems or Internet banking breakdowns, can be listed similarly to other banks around the world.

A small part of the total annual losses from international banks comes from Operational risk but when a non-expected event happens then banks have significant. For this reason, and due to the fact that there are a lot of changes in the world-wide banking industry, financial globalization and local regulations, better policies and recommendations concerning with operational risk management are being obtained. Additionally, an appropriate operational management in the international banking sector may minimize the possibility of bankruptcy and infection.

In the academic literature on operational risk in the financial segment there are different point of views from several authors, and some of them are often inconsistent (Acharyya 2010, Moosa 2007).

According to Mossa (2007), Operational risks have three dimensions, the cause, the event, and the consequence. Data Operational Risk data exchange Association mentioned the Operational risks events connected with the International Banking Sector as follow:

- External frauds:
    a) Fraud and theft: these are losses caused by a fraudulent act, deceptive property or avoidance of the law by a third party without the assistance of bank staff.
    b) Security systems: events related to unauthorized access to electronic data files.

- Internal frauds:
    a) Fraud and theft: losses due to fraudulent acts, unsuitable credit of goods or tax evasion of regulation or business policy, involving the involvement of internal staff.

b) Unauthorized activities: these are losses from unreported planned and unauthorized operations, or purposely unregistered positions.
c) Security systems: all events relating unauthorized access to electronic data files for personal profit with the assistance of employee's access.

- Malicious damage: Losses caused by deliberate damage, terrorism, external and internal security systems.
- Labor practices and workplace
- Customers, products and business practice Business
- Disasters and accidents
- Technology and infrastructure failure like hardware, software and telecommunications malfunctioning, failures in management processes.

The lack of attention to operational risk management is one of the main reason of the main failures at banks (Hess. 2011). Consequently, operational loss can happen at all levels of organization, from board of directors until colluding groups of people (Jongh et. al., 2013). External risks are easier to identify than loss from internal events which are most often connected to the activities of the bank. Financial Companies investing in managing risk by allocate resources to risk management operations. Basel II is a regulator for banks, focusing in operational risk (Chavez-Demoulin, 2006). Basel II (2006) is a framework provides instructions for operational risk for banks and financial institutions. The regulation of Basel II contains identification, measurement, monitoring, reporting, control and mitigation of operational risk.

2.4.5.1. Basel Accord of Operational Risk

The most important financial institution of banking supervision and bank's risk management is the Basel Committee on Banking Supervision (BCBS). The Basel Capital Accord (Basel II) was published in January 2001but its final version was released in 2004. The advanced version of Basel II was issued in 2006.

According to Manic (2008): "BCBS tends to find the best common approaches and common standards for every member country in order to promote the advancement of risk management in the banking system, strengthen banking

supervisory frameworks and to improve financial reporting standards. To achieve this, BCBS has published many documents in the field of capital adequacy, banking problems, accounting and auditing, core principles for effective banking supervision, credit risk and securitization, market risk, operational risk, money laundering and terrorist financing, transparency and disclosure. For the risk management, the most important documents are the Basel Accords, Basel I and Basel II".

The first Basel I was focused on market and credit risk. Basel II, an improvement version of Basel I, was focused on the operational risk. The main goal of Basel II to help to increase the safety and soundness in Banking sector (Basel Committee on Banking Supervision, 2006).

Basel committee's (Basel II) capital accord (BCBS, 2006) suggests three methods for operational risk capital calculation. These are:

- Basic indicator approach (BIA)
- The standardized approach (TSA) and
- Advanced measurement approach (AMA)

Further, in Basel II categorized seven Level 1 event types which are the types of incidents that will be used to calculate operational risk (BCBS, 2006). It is very important when defining an event to analyzing its impact and the likelihood of it happening again.

The level 1 event types are:

- Internal fraud
- External fraud
- Employment practices and workplace safety
- Customers, Products and Commercial Practices
- Damage to physical assets
- Business disruption & system failures

- Execution, delivery and Process Management

Every bank can implement an internal sub level based on Basel regulations.

2.5. Cyber Threats –Risk

The stability of our global network and the well-functioning of our countries, cities and everyday activities are based on the Internet. Critical infrastructures, including transport, transport safety, nuclear power stations, electricity and communication networks, have potentially devastating consequences for humanity. Cyberspace is at risk from its nature as a penetrating, multi-layered and multi-layer threat, with no visible weapons or attributed actors (Stauffacher, Sibilia & Weekes 2001). Most cyberattacks, do not directly target lives, but the organized vandalism of cyberattacks but this could be developed to something more serious if it prevents a society from meeting basic needs (Lin, Allhoff & Rowe, 2012).

Europol stated that the use of internet, in recent years, has significantly enabled communication and promoted global development and communication but at the same time has caused new, modern challenges in the form of cybercrime as criminal groups exploit these technological advantages. Furthermore, Europol reported that the biggest security threats that European Union deals with come from terrorism, international drug trafficking and money laundering, organized fraud, counterfeiting of the euro currency and people trafficking. Europol argued (2011) that the value of the cybercriminal economy is not known, the estimated global corporate losses are approximately 750 billion Euros per year. (Europol Public Information 2011).

According to Howard & Longstaff (1998) an attack is several tasks taken by an attacker to achieve an unauthorized result, which in not approved by the owner or administrator. The systems weaknesses and vulnerabilities is a result of cyber threats. Cyber security as information security involves three core principles (Johnson, 2010, Brunette & Mogull, 2009, Greene, 2006, Whitman & Mattord, 2004):

- Confidentiality – protecting
- Integrity – maintaining
- Availability - ensuring.

According to Rufi (2006) these three principles are unfocussed by:

- Misconfigured hardware or software
- Poor network design
- Technology weaknesses
- End-user carelessness
- Intentional end-user acts.

These threats can be identified to minimize the risk but risk cannot be eliminated

There are seven groups which cyber threats can be divided, according to Thuraisingham (2005):

- Authentication violations
- Nonrepudiation
- Trojan horses and viruses
- Sabotage;
- Fraud
- Denial of service and infrastructure attacks
- Natural disasters

According to Jayawickrama (2008) cybercrime is motivated by some aspects:

- Economic benefits – personal and/or organizational financial gains,
- Power – desire to impact large systems and organizations,
- Revenge – desire to impose loss or damage
- Adventure
- Ideology – desire to express,
- Desire – self-indulgence.

Furthermore, researchers Gandhi, Sharma, Mahoney, Sousan, Zhu and Laplante (2011) stated that cyberattacks included in four groups by motivations – social, political, economic and cultural.

Ponemon Institute (2013) which annually provides cross-country and cross-industry information (Ponemon, 2013) finds that security and data breaches has a result an average financial impact of US$9.4 million in 2013 (Greisiger,2013). The global economic impact of cybercrime, according to McAfee calculated at US$300 billion to US$1 trillion (McAfee, 2013) In 2009 a report for the World Economic Forum (2012) represent the total economic losses from cybercrime to be more than US$500 million.

2.5.1. Definition

Furthermore, "cyber risk" can be refer to various sources of risk which affects the information and technology profits of a firm. The term Cyber risk was defined as the risk which creates malicious electronic events that has as result disruption of business and loss (Mukhopadhyay et al, 2005)

The term cyber includes all digital networks which are essential for storage, modification and communication of information (European Commission, 2012).

According to the German Federal Office for Information Security (2012), there are differences between the definition of cybercrime and cyber risk. Cybercrime involves of criminal acts in contradiction of the Internet or other data networks, computer systems or their data, and crimes committed through such information technologies. While cyberspace includes attacks and turbulences, the term cybercrime is limited to cyberattacks, targeting and targeted cyberattacks (Bundeskriminalamt, 2012)

Cybercrime is described as all criminal activities that use modern information technology, such as computer technology, network technology. Cybercrimes can be separated in illegal access, illegal interception, data interference, systems interference, misapplication of devices, forgery electronic fraud (Moore, 2005).

The term cybercrime is about all criminal behavior which involve a computer or network.

Cyber risk has been defined as connection of malicious electronic events (Mukhopadhyay et al., 2013). Cyber Risk can be used as synonym of information security (Öğüt et al., 2011). Some authors categorize the cyber risks as operational risk (Biener et al., 2015, Cebula and Young 2010). Operational cyber threats addressed into four cyber security risks, which contains: actions of people, systems and technology failures, failed internal processes and external events (Ehlert,Rebahi,Magedanz, 2009).

2.5.2. Common Cyber Threats for Banking Industry

In 2016 Price Water House Coopers published a Global Economic Crime Survey where cybercrime was the second most reported crime globally and that 54% of organizations have deal with cybercrime incidents in the last two years. One of the main business sectors that was target for cybercrime is banks. The last few years more and more incidents have reported with banks from all over the world been hacked. Some of the recent attacks are when hackers attacked the Tesco bank and stole over £2 million from customer accounts, DDoS attacks in HSBC and the phishing scams in banks in UK which has a target the banks customers (Ismail Nick, 2017). Below is a list with all the cyber threats that a bank can be hit:

- Spamming

Spamming usually refers to the abuse of electronic messaging systems and the indiscriminate sending of unsolicited bulk messages (Ollman, 2006). Spamming includes the e-mail spams, instant messaging, web search engines, internet forums, blogs, and mobile phone messages. People who using spamming have as goal the fraud, to spread all kinds of viruses and malicious software for identity theft, distributing malwares.

- Denial of service (DoS)

A DoS or Distressed DoS attack (DDoS) is a crime that makes computers or network resources inaccessible to users or their customers. Every criminal who use DoS has different means, incentives and goals. DoS can be described as the concerted, malicious attempts of a person or persons to make a website or service impossible to perform normally or not at all (Yuval F., Uri K., Yuval E, Shlomi D and Chanan G, 2010). Criminals are always interested in websites or servers that are associated with high-profile servers, such as banks, credit card payment gateways, and even root-based DNS servers (Yuval F., Uri K., Yuval E, Shlomi D and Chanan G, 2010). According the Computer Emergency Readiness Team the symptoms of DoS attacks include the following (McDowell, 2008):

- Unusually slow performance of network services,
- A website is unavailable and
- An increasing number of spam e-mails.
- Malwares

Malware refers to software that is designed to infiltrate or destroy a computer system without the owner's knowledge. The word malware combines the words malware and the software. Computer professional defined it as all kinds of software or program codes with hostile or disturbing purpose. Malware includes computer viruses, worms, Trojan horses, dishonest adware, and other malicious and unwanted software (Joint Commission on Technology and Science, 2005)

- Hacker

Hacker is someone who tries to investigate systems or gain unauthorized access to others' computers through specific skills or knowledge (Sterling, 1993). There are usually three types of hacker: black hat hacker, white hat hacker and hacker hat (Sterling, 1993). Most common type of hacker is black hat hacker that is malicious or criminal (Sterling, 1993). White hat hackers are moral hackers and those who are doubtful in ethics are called gray captains of hackers.

- Phishing

In computing, phishing refers to attempts to criminally and fraudulently gain sensitive information, such as usernames, passwords, and credit card details, by means of some public entities that run on electronic directs users to enter their detailed information on the Web site). These days, efforts have been made to protect people from phishing, including law, user training, and technical measures. The phishing technique has been used since 1987, and the first reported phishing was in 1996, although the term existed on hacker-related print publications even earlier (Felix J. and Hauck C., 1987 Paget F, 2007). The last few years the reports about phishing are increasing dramatically. This kind of crimes have been more likely to target customers of banks and payment services. Another type of phishing attack is via E-mail, to steal customers' sensitive information. Further, phishers send e-mails indiscriminately to many people expecting some to respond. Afterward, criminals determine which bank the users used and begin to send bogus e-mails, responsively. Phishers also target social networks, through which they can gain a customer's personal information for identity theft (Felix J. and Hauck C., 1987). These kind attacks have reached a success rate of over 70%.

Identity theft is a term used to describe fraud in which the criminal pretends to be someone else to steal money or get other benefits. It is also a crime for criminals to pretend to be someone else even if they do not steal an identity (Felix J. and Hauck C., 1987).

Phishing refers to attempts to obtain sensitive information, such as user names, passwords and credit card details, through some publicly-owned online operators that direct users to enter their detailed information into site. Efforts have now been made to protect people from electronic fishing, including legislation, user training and technical measures. This technique has been used from1987 but the first report for phishing was in 1996, although the term existed in hacker-related articles even earlier (Felix J. and Hauck C, 1987 Paget F, 2007). E-fishing reports have increased dramatically. Recently, these crimes are

more likely to appeal to banking and payment customers. Another technique of phishing for stealing sensitive customer information is Email. Firstly, phishers send e-mail messages to many people waiting to respond. Criminals then determine which bank users use and begin to send false emails. Furthermore, Phishers through social networks through can obtain customer identity information about identity theft (Felix J. and Hauck C., 1987).

According to the US Federal Trade Commission, every year in the USA, approximately 10million people are victims of identity fraud (Paget F., 2010). Mostly, such crimes are related to computer theft, loss of backups, or compromised information systems and are intended to reap financial benefits or to conceal illegal activities by using a legal identity (Paget F., 2010).
Generally, the penetration into a bank's systems is often seen as the greatest threat because of the ability of the malicious actor not only to steal data but to modify or delete it. Hackers can gain administrative control over networks that, if circumvented, can cause disastrous consequences, by exploiting software, hardware or human vulnerabilities. If disclosed, network security breaches may affect stock prices, cause irreparable damage to reputation, and affect the stability of the wider financial market.

2.5.3 The Impact of Cyber Attacks

The ongoing digitalization, which evolves providing to customers new service opportunities drives cybercrime increase and banks are expose to more complex methods of attack. The last few years there are reported a large number of attacks in banking sector, comprised stealing money to restricting online payment systems such as online banking through websites, mobile apps. The type of Cyberattacks in the banking sector are related mostly to fraud, due to the financial gain and have many forms (Arachchilage et al., 2014: NCSC, 2014; Lagazio et al., 2014; Bhasin, 2007).

Furthermore, banks dealing with phishing incidents very often (Manzoor, 2014). With the use of Phishing, Malware and Skimming criminals steal confidential information such as online banking details, customer's card information and

personal identification numbers from its victims (Arachchilage et al., 2014, Choo, 2011). Besides phishing, malware and skimming, a Distributed Denial of Service attack (DDoS attack) is another risk that banks deal with (Bhasin, 2007). When a service, for example bank's website, becomes unavailable this is considered as DDos attacks (NCSC, 2014).

Cybercrime is a significant risk exposure for both, individuals and organizations. The effect to this exposure comprises financial losses, regulatory issues, data breach liabilities, damage to brand and reputation, and loss of client and public confidence (Verma, Hussain and Kushwah, 2012). Therefore, cyberattacks can seriously threaten the finances and reputation of banks and it also affects the relationship between the image of the organization and the trust that customers and other stakeholders have in the organization. When an organization become victims of cybercrime, has as a result negative publicity which creates serious problems (De Joode, 2011).

2.5.4. Cyber Risk Management

When banks are challenged with cybercrime, crises can occur. According to Coombs (1999) "Organizational crisis is an event that is an unpredictable, major threat that can have a negative effect on the organization, industry, or stakeholders if handled improperly" (Coops, 1999, p. 2). Crisis can be avoided or treated if there is an organization plan. The first step of the risk management is Risk Identification.

This step is very important in order to manage the risk. In the Risk Identification banks need to provide information on their business model, for identifying valuable firm resources (ISO/IEC 27005). Valuable resources, are very important for business operability and can contain data information, software, physical assets or General IT infrastructure, employees, services and other intangible assets (ISO/IEC 27000).

Companies should also identify the importance and dependency of their core business on the cyber environment. Therefore, banks should identify its need for

information security and determine the requirements and decide for the level of information and IT security (ISO/IEC 27001 and 27005). The next step is a comprehensive risk identification. The process of identifying the cyber threat should include vulnerabilities, existing risk controls and the consequences of breaches of security (ISO /IEC 27005).

The next step of the risk management process is Risk assessment and valuation After the identification of cyber risks, organization must assess and quantify the risk. Organizations needs to assess the possible losses and impact probabilities of cyber risks (ISO/IEC 27001 and 27005). The risk assessment procedure contains the realistic estimation of consequences of cyber risks, the probabilities when these risks occurs and the assessment of the general risk level. Finally, the decision as to whether risks are acceptable or if risk response measures are required has to be made by the management.

After the Risk Assessment, the Risk response measures must be applied. Risk response can be established by risk avoidance, risk mitigation, risk transfer or risk acceptance. With the use of this methods you can minimize the losses for the organization but you cannot eliminate the risk. According to ISO/IEC 27001, some controls tools that a company can apply to minimize the risk are access control, cryptography or physical and environmental security.

The next step of risk management is Risk control. After the identification, assessment and valuation and the risk response measures of cyber risks, risk control is the following step. In the process of the risk control, companies should make an ongoing review of the risk, monitor their risks and adjust or improve the control measures if it's necessary (ISO/IEC 27001).

Additionally, Miller (2009) described three stages in which organizational crisis can evolve: pre-crisis, crisis, and post crisis.

The Pre-crisis stage, is the stage where the employees, organizations and stakeholders, work to prevent and prepare for a possible crisis (Coombs, 2007; Miller, 2009). In the case of the banks, they implement cyber security measures

to protect information. With Cyber security organization can achieve good reputation and limit the actual occurrence of incidents and the damage they cause. Computer threats and individuals' predictable behaviors have as a result cybercrimes, thus, it is important for an organization to fight cybercrime using both technological and conventional behavioral counter measures (Arachchilage et al, 2013, Arachchilage et al., 2014, Lai, Li and, Hsieh, 2012, Metalidou, Marinagi, Trivellas, Eberhagen, Skourlas and Giannakopoulos, 2014). The impact of Cybercrime to an organization is the continuity of business processes, reputation, cost and liability of protecting customer or personal data and risk management (De Joode, 2011, NCSC, 2014).

Furthermore, banks can use technological solutions such as basic protection- and defensive measures (Bhasin, 2007). Secondly, employees must recognize and assess risks and know which measures should be taken to reduce risks and errors. In order employees to be able to aware the type of risks, a bank could provide them with seminars, or trainings (NCSC, 2014, De Joode, 2011, Bhasin, 2007). Moreover, banks can inform their customer and create awareness among them, by providing them general clarification on their websites about how criminals perform attacks, what security measures the bank has applied and how customers can secure their devices and confidential information as effectively as possible.

When a crisis is in placed then there is a trigger that organization's survival or reputation is at risk (Miller, 2009) and managers must respond to this crisis (Coombs, 2007). The banks should be well prepared for a cyber incident by having an incident response plan as part of their policies and procedures. Having this plan, banks can limit the damage to their image and reputation (Coombs, 2006, Bhasin, 2007). During a crisis, there is a lot of uncertainty (Miller, 2009), so is very important to keep customers trust and protect organizations reputation with using significant actions and clear communication (Coombs, 2006).

Last, in Post crisis stage, organizations are returning to business as usual. In the post crisis stage, there are some basic activities that need to be explored. First, executives should provide all the information to the bank's customers and other stakeholders as soon as this information is known. Secondly, to inform stakeholders about the progress of recovery efforts and, finally, to evaluate and analyze the crisis. It is important stage because you can understand why the crisis happened, learn from the crisis and integrate these lessons into the organization's crisis management system (Coombs, 2007).

2.6. External Fraud

Fraud is a major incident for all banks worldwide, even if different measures have been taken to minimize the fraud cases, it still arise. (Rezaee, 2004). In fraudulent cases, the people who commit fraud have enormous gains and the likelihood of apprehension and thus of conviction and punishment is minimal (Cain, 1999).

The bank fraud can be separated into two groups according to Alashi (1994), institutional factors and environmental factors. The factors that are found in the financial sectors internal environment are called Institutional factors, while the factors that come from the impact of the environment on the financial industry are the environmental factors. Among the main reasons are the volume of work, the nature of the services, and the banking experience of the staff, the poor security, insufficient infrastructure, the delays in gathering documents and the lack of effective deterrence - punishment. Banking fraud may also be committed from outside the bank, or external fraud.

One of external fraud type is the ‘new account fraud’, which a criminal use a fake or stolen identity to open a new account, to obtain a credit card or loan (Hartmann-Wendels, Mählmann, & Versen, 2009).External fraud is considered when an outsider can penetrate the security of that bank's data and gain access to sensitive information or fraudulent transactions. There are a number of ways that can be achieved such as bad password security may allow a scammer to gain access to the bank's information systems without the need for sophisticated

computer piracy, or stolen customer information, including bank and credit card electronic data. Theft of confidential data is detrimental to a bank's reputation even if there is no direct financial loss as a result. External partners are usually based on assistance and collusion by bank employees - who may have been paid relatively small amounts to facilitate crime Additional, a type of external fraud is existing account fraud, where the criminal has access to an existing account or set of accounts and uses them for fraudulent purposes, this can happen in cases of hacking, phishing, and scams. According to Hartmann –Wendels et al. (2009), existing account fraud are easier to detect than new account fraud, especially if the fraudster continues to have the account legally for some time (Hartmann-Wendels et al., 2009). Identifying fraud is often done informally, which reduces the potential for a cost-benefit analysis to determine appropriate systems for detection (Canhoto & Backhouse, 2007).

2.6.1. Definition

A worldwide phenomenon which affects all sectors of the economy is Fraud. The Institute of Internal Auditors' "International Professional Practices Framework (IPPF) defines fraud as: "Any illegal act characterized by deceit, concealment, or violation of trust. These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by parties and organizations to obtain money, property, or services; to avoid payment or loss of services, or to secure personal or business advantage." A Fraud incident can impacts organizations in different areas including financial, operational, and psychological. Fraud is defined as the intentional act of one or more persons, between employees of an organization or third parties, which results false in the financial statements (Adeniyi, 2004).

According to Fraud Act (2006), the frauds definition includes the false representation, the failure to disclose information, and the abuse of position. Furthermore, the Federal Bureau of Investigation (FBI) in the United States stated that fraud is an illegal act which is characterized by dishonesty, disguise or violation of trust and which does not necessarily includes either threat of

physical force or violence, but comprises the terms of lying, stealing and cheating (Silverstone et al., 2012).

Silverstone and Davia (2005) have separate the term Fraud into three primary groups: fraud that has been exposed and is widely known, fraud that has been discovered by organizations but not made public yet, and fraud that has not been detected. Research addressed that approximately 20% of fraud belongs to the group of exposed fraud because most fraud incidents are discovered accidentally, independent auditors do not proactively audit to detect fraud, staff is not trained or have the experience to notice fraud proactively ,most internal controls are insufficient to prevent fraud (Silverstone and Davia, 2005; Wells, 2004; Albrecht, 2004).

Moreover, another categorization of fraud comes from Elliot and Willingham (1980) who categorized fraud into two groups the management fraud and employee fraud. Management fraud is committed by managerial employees and includes perversion of material facts, stealing of assets, and disguise of material facts, illegal acts, corruption, and conflict of interest (Silverstone and Sheetz, 2004). This kind of fraud has as result stock prices, management bonuses, availability and terms of debt financing (Silverstone and Sheetz, 2004).

On the other hand employee fraud, committed by non-managerial employees and involves misappropriation, breach of confidential duties (Elliot and Willingham, 1980). The fraud incidents are committed in order, individuals and organizations, property, or services, to gain money, to secure personal or business advantage to avoid the payment or loss of money or services, (Silverstone and Sheetz, 2004). Consequently, Fraud involves criminal crimes which imply the use of deception for personal gain at the expense or loss of another person. The activities that included to this incident are deception, bribery, theft, embezzlement, forgery, collusion, conspiracy, money laundering, blackmailing and hiding of major events (Chartered Institute of Management Accountants, 2008; Theft Act, 1978; Fraud Act, 2006).

The definition of bank fraud is a conscious or thoughtful attempt to achieve an illegal financial advantage against another person who is the legal owner of the fund (Orjih, 1998). During a Bank fraud, there is a loss of assets by banks through fraudulent and dishonest means. The fraudster has a goal to reward himself against the banking or banking staff or the banking client or any member of the public through bank operations. A-Fraud can be committed by bank customers, bank staff, or a combination of staff and client or non-customers. Generally, banks refused to publish details of the frauds they may have committed in their banks because they fear that they will lose their corporate image (Eze, 2004).

The first type of bank fraud is the internal fraud, which is committed by a member of the bank's staff (Greenbaum & Thakor, 2007). The second type of fraud is external fraud. According to Basel Committee (2006) definition, external fraud is the losses from a fraud incident because of stealing or avoidance of the regulations by the third party and includes theft, robbery – forgery, hacking. External Fraud in the bank can be committed by customers, suppliers, and even ex-employees and can result from the theft of personal data of legitimate clients of the bank or by forgery of personal data in order to increase the likelihood of lending to customers who otherwise would not qualify (Mishkin, 2006).

2.6.2 Theories of Fraud

Fraud has become one of the biggest threats to the global economy and this global problem impacts the financial institutions. Many organizations do not recognize that fraud can prove even more destructive than other forms of critical incidents such as terrorist attack, fire or floods. Such events can cause serious business disruption, undermines financial stability, damage to reputation and loss of investor confidence that it proves to be irreparable.

Hence, over the year a number of fraud theories have developed to explain the term fraud such as Fraud Triangle Theory (Cressey, 1973), Theory of differential association, Job dissatisfaction theory (Hollinger and Clarke, 1983), The fraud scale, The fraud diamond theory, Eclectic Theories.

2.6.2.1. Fraud Triangle Theory

Donald Cressey in 1973 published the most widely accepted fraud theory. Cressey's theory was named Fraud Triangle Theory. The triangle represents three factors the individual's pressure, the opportunity and rationalization for committing fraud. The first factor, the pressure on the employee, is due to 'non - shareable' economic problems. The definition that Cressey (1973) gave to fraud is that fraud is a result of the problems the person has realized is somewhat inconsiderable. He identified six types of non- shareable problems that were believed to lead to the possibility of fraud in the individual. Furthermore, he considered the term "non- shareable" as relative, varying from person to person (Cressey, 1973). In addition to this, what cannot be distributed to an individual cannot be distributed to another. Moreover, non-shareable issues were related to status-seeking or status maintenance activities. The six categories of non-shared problems include breaches of obligations, personal failures, business upheavals, isolation from friends and associates, requirements that are required, and problems in employers/employees relationship (Cressey, 1973). Opportunity is the second factor of the Fraud Triangle.

A problem that it does not share will not lead an employee to commit fraud (Wells, 2005). An employee can commit the crime without being caught. Even if the position of trust can provide an opportunity to solve an undisclosed economic problem, Cressey (1973) found that many of the employees that have positions which provide them trust and this position offered them opportunities didn't originally involve in fraud using money allocated to solve their problems. Wells (2004) stated that the very essence of a person's trustworthiness implies that, since the position is confidential, it may be dishonored. Opportunities could be presented in the form of poor political discipline or poor organizational ethics and poor internal controls, (Cressey, 1973, Wells, 2004).

Rationalization is the third factor of Cressey's theory. The act of rationalization is not a retrospective thought that justifies fraud, but it is the reason that a person acts in a fraudulent way. Hence, Rationalization is an incentive for

committing fraud and is often abandoned after the crime has been committed (Wells, 2005).

For many years, Cresset's Fraud Triangle has been used to explain the nature of fraudsters Cressey (1973) stated that the theory of the fraud triangle is limited to its practical use to prevent and detect a breach of trust, such as fraud or the treatment of arrested perpetrators.

2.6.2.2. Theory of Differential Association

One of the first theories of fraud was the one that Edwin Sutherland developed in the 1930's, "Theory of Differential Association". According to Wells (2005), Sutherland can be said to be the "Father of white-collar crime. His first research was about the fraud committer from senior business executives against shareholders or the public and he invented the term "white-collar crime" in 1939.

Sutherland suggested in his Theory of Differential Association Sutherland (1949) that crime is learned. He believed that criminal behavior has been made with other people in a communication process and therefore crime cannot happen without the help of other people. Sutherland (1949) considers that criminal behavior occurs when a person is more exposed to definitions that favor a violation of the law than to definitions that are unfavorable to the violation of law. Consequently, criminal behavior is a consequence of contradictory values. He believed that the learning process consists of two areas: the techniques for committing crime and the attitudes, movements, rationalities and motives of the criminal mind. Therefore, he found that organizations with dishonest employees would eventually "infect" some of the honest people and generally that honest workers would ultimately have some influence on some of them who are dishonest (Sutherland, 1949, Wells, 2005).

2.6.2.3. Job dissatisfaction theory

In 1983 the results of research by Hollinger and Clarke on 12,000 employees was that dissatisfaction motivated employees can commit fraud. When workers

realized that their work or working conditions were unfair, they were more likely to commit fraud (Wells, 2005). However, this theory is difficult to prove due to the relative lack of information about the theft of workers and the lack of reliable and widely used information about the theft of workers (Mustaine & Tewksbury, 2002).

2.6.2.4. The fraud scale

'Fraud Scale' was developed by Steven Albrecht (Albrecht et al., 1983) in the 1980s' and has common factors with Cressey's (1973) in explaining criminal behavior. Fraud Scale theory suggested that there are three factors consist to fraud: a situational pressure, a perceived opportunity to cover the fraud and, the level of the employees' personal honesty. Situations pressures are defined as the immediate problems faced by individuals in their environment. Fraud opportunities can be created by individuals or by incomplete internal control. Personal integrity is has been described as the personal code of ethical conduct that each person adopts. According to Albrecht when situational pressures and apparent opportunities are high and personal integrity is low, work-related fraud is much more likely to occur than when the opposite is true (Albrecht, Howe and Romney, 1983).

2.6.2.5. The fraud diamond theory

The Fraud diamond theory was developed by Wolfe and Hermanson (2004), and includes four elements. This theory suggested that in order a fraud event to be occurred requires motivation, opportunity, rationalization, the capability of committing the crime. Capability includes the technical knowledge, confidence to perform and get away with the crime (Wolfe & Hermanson, 2004).

2.6.2.6. Eclectic Theories

There are some theories of fraud named selective, which present a combination of factors involved in creating the intention to commit fraud:

- Fraud in the Accounting Environment DEVELOP by Riahi-Belkaoui and Picur (2000), which suggested a framework for fraud in the accounting environment.
- Anomie Theories, focus on the confusion that arises in an individual when there is a weakness between values and rules. In an effort to align the objectives with the means, one person can adopt five types of solutions, including compliance, innovation (using illegal means of success, such as accounting fraud), ritualism, revivalism and rebellion (Durkheim, 1964, Merton, 1938, Merton, 1957). All these adjustments happen from the pressures of society that aggravate economic success and the difficulty of achieving it. Accordingly, theories of anomie comprise failure to connect the rules or values of goals with the ability to implement the goals using illegal means (Durkheim, 1964, Merton, 1938, Merton, 1957).

2.6.3. Types of External Fraud in Banking Industry

External Fraud is related with incidents that their committed by persons not connected with the bank. A common example of external fraud is a robbery attack either during the banking hours or during special movement of cash in transit. Moreover, some external frauds could arise from carelessness and carelessness or negligence on the part of some customers or when a dishonest staff can access the company's checkbook. There are various types of fraud committed by individuals and organizations outside the bank, with or without the involvement of bank staff, individuals who might be bank customers or those who do not cooperate with these banks. These types of External Fraud in Banking Sector are:

- Over-invoicing: The pricing of services provided to banks is made by doubtful supplier, either by inflation of normal interest rates versus the actual value of the services provided or bank employees must pay for services already paid. (Omachonu, and Ndulor 1998; Idowu, 2009).
- Advance fee fraud: This may include an agent approaching a bank with an offer of access to large funds often on a long-term basis. The source of such

funds is not specifically defined and the way to access it (Omachonu, and Ndulor 1998).

- Account Opening Fraud: It usually begins when a person who is not known to the bank asks to open a trading account, such as current and savings account with a false identity but unknown to the bank and starts to deposit and withdrawal fraudulent cheques.
- Money Transfer Fraud: Money transfer services are means of transferring funds from one bank to another bank worldwide. A fraudulent transfer of money may arise from a request created solely for the purpose of committing a fraud or making an amendment to the request for transferring money by changing the name or account number of the payee or changing the amount of the transfer
- Cheque Fraud: Used as a payment instrument or for payment of financial obligations. Typical types of checks are personal, business, government travelers, certified designs, and controls, each having its own features and vulnerabilities for fraudulent use. Most common scams include checks that are stolen, forged, or tampered with.
- Loan fraud: Part of the traditional services of financial institutions are the loan and other forms of credit facilities In the process of credit facility, fraud can occur at any stage, from the first interaction between the customer and the bank until the final payment of the loan. Loan fraud occurs when the facility is extended borrower who has exceeded their credit limit or the facility is given to a new or existing customer of the bank who is not appropriate candidate for granting a loan. (Omachonu, and Ndulor 1998).
- Money Laundering Fraud: This is a means of where money that comes to the bank has unknown source or fund that have illegally received are converting to cash into non-traceable transactions in banks. The cash is disguised to make the income legitimate (Umunna, 1989).

2.6.4. Causes of Fraud

Different researchers have explored and defined the causes of fraud. Shongotola (1994), grouped the main causes of fraud into two categories: The Institutional

Factors and The Environmental / Societal Factors. Institutional factors can be defined as the factors that banks found in their internal environment and environmental or social factors are those are depended from the impact of the environment or society in the banking industry.

According to Shongotola (1994), Institutional causes of fraud are categorized as:

- The volume of work: The volume of work is large so employee might have not to be aware that the documents have not been signed and have proceeded
- Number of Staff: When an employee manages a large number of staff, there is a strong chance that fraud could not be perceived.
- Nature of Services: Fraud may be caused when value documents and cash are exposed to unauthorized personnel or unauthorized persons, for example, customers.
- Banking Experience of Staff: Fraud in banks appears more frequently in staff with little experience and knowledge of the financial practice. The more a person's experience and knowledge are, the less likely the fraud will pass from this staff if there is no active support from the staff.
- Inadequate Staff Training: This could affect the morally weak as well as the powerful strong staff in various ways. The lack of knowledge on how to deal with fraudulent practices in banks could affect the staff. Banks with poor management record a higher incidence of fraud than any of those with efficient management. Poor management leads to an inefficient and inadequate control system and indifference between staff.
- Staff Negligence: The negligence of the staff could lead to fraud in commercial banks. The negligence can be affected for many factors, such as bad supervision, lack of technical knowledge, apathy and pressure, and lack of experience.

According to Shongotola (1994), the Environmental causes of fraud are:

- Personality profile of dramatizing personnel: Most people with excessive with ambitions are prone to fraud. These types of people tend to earn money with scams.
- Societal Value: According to Fagbami (1990), the system of values in every society is the set of rules that define what is right or wrong in this society. The undermining of social values and the growing social expectations of bank staff or any people connected or not to the bank and the subsequent desire of all them to meet these expectations are also factors contributing to fraud.
- Slow and Tortuous Legal Process: Delays in prosecuting fraud cases can result abandon the case in the middle and not achieving justice.
- Lack of Effective Deterrence & Punishment: The lack of an effective deterrent, such as heavy punishment, could be a contributing factor to non-synergy in committing fraud to banks.
- Fear of Negative Publicity in Reporting Fraud Cases: Many commercial banks do not report fraud to the authorities. They believe that this will give unnecessary negative publicity. This behavior encourages people who commit fraud.

2.6.5. External Fraud Management

The fraud management lifecycle can be used to help the process of fraud prevention (Wilhelm, 2004). This fraud management cycle contains eight stages:

- Deterrence
- Prevention
- Detection
- Mitigation
- Analysis
- Policy
- Investigation and
- Prosecution (Wilhelm, 2004).

The first stage of deterrence stage includes activities that prevent or discourage fraud with fear of consequences (Wilhelm, 2004, Webster, 1997, 1976, 1941). Prevention activities prevent, control, hold away or prevent fraudulent activities. The detection stage reveals an existing or attempted fraud. In any fraud management system, the process of fraud detection and prevention is vital. Fraud detection is extremely complex and a high percentage of cases of fraud are actually found external or by an accident (Dyck, Morse, & Zingales, 2007).Thus, methods such as monitoring and life cycle verification can be used to reduce the overall incidence of fraud (Potter, 2002; Porter, 2003; Wilhelm, 2004; Venkatraman & Delpachitra, 2008). According to Suh and Han (2002), to build trust between bank and customers, it is crucial to use effective fraud prevention measures to prevent customer fraud.

Mitigation includes activities aimed at stopping fraud, like blocking access to the bank account. Freddie Mac (2015), stated that "Fraud Mitigation Best Practices" contains: (a) Fraud Risk Management Policies and Procedures:

Enforce appropriate policies and procedures for detecting, preventing, investigating, resolving and reporting fraud and communicating to employees. (b) Regulatory Compliance: Make sure that appropriate policies and procedures apply to your company's obligations, (c) Ethical Conduct: Inform employees with your company's ethical standards (d) New Employee Awareness: New employees should be informed of the fraud awareness during the orientation programs and (e) Training: Ensure that workers receive appropriate training about fraud.

The analysis stage seeks to identify the underlying cause of fraud and the factors that have led to the occurrence of the fraudulent activity. In the sixth stage, it is very important to create evaluate and communicate policies that aimed to reduce fraud, for example, the setting of limits in the authorization such as any transaction over € 10,000 must be reported (Mativat and Tremblay, 1997). The seventh stage of the survey gathers data and information to deal with the

fraudulent activity, asset recovery or safe restoration, and collect the evidence necessary to successfully prosecute fraudsters.

The prosecution is the final stage of Fraud Life Cycle Management and involves the conclusion of all the successes and failures of the life cycle of fraud. There are failures due to the fact fraud was successful and successes because fraud was detected, a suspect identified, arrested and accused. The stage of the prosecution comprises the recovery of assets, the repayment and the conviction with the corresponding warning value (Mena, 2002). Furthermore, many known frauds are not prosecuted because of concerns about the damage will be caused to the image and reputation of the organization. The combination of internal factors (information technology, risk tolerance, fraud management philosophy.) and external factors (regulatory requirements, competitors, and fraud methods) contribute to the fight against fraud.

2.7. Business Continuity

Business continuity has its roots in disaster recovery, which occurred in the 1950s and 1960s as companies started to store back-ups of their critical data, paper or e-mail, in alternative locations. Initially, periodically, off-site backup and storage procedures have become more common and regular since the 1970's when a handful of third-party storage facilities created what would be an alternative site or a "hot site" purchase. The recovery from disasters came to its own in the 1980s when the market for alternative places grew significantly. The hot site has become a very popular disaster recovery solution for data-driven financial businesses with large central hosts.

In 1983, the Federal Office of the Currency Controller (OCC) instructed financial institutions to develop documented recovery plans. With non-specific instructions, the directive was largely considered to be the only backup and data recovery. Compliance, for the most part, came in the form of transferring backup tapes to locations out of storage. In 1989 Federal Financial Institutions Review Council (FFIEC), tested the rehabilitation plans, this was the best documentation and maintenance.

The 1990s it was the biggest IT revolution and affect the disaster recovery industry. Computers were ubiquitous and most companies acquired huge servers and desktops distributed throughout the organization. This changed the game to a post-disaster recovery. By the end of the 1990s, the term "continuous operation" has become a popular replacement of the term recovery, as recovery developers seek to mitigate a whole host of vulnerabilities, from human error to network failures and invasion of communications failures emerged from this decentralized computing environment. The disaster recovery term was used to describe the traditional IT and data recovery issues, and business follow-up was the term that describes the need for continuity across the enterprise, from facilities to communications.

At the end of 1990's, the Business Continuity Management came forward. Though, Business Continuity Management gained significant recognition within organizations after the events of 9/11 (Yankee Group, 2001).

Organizations that had a plan during this disaster could continue business very quickly, while those who had no plans soon broke down. After September 11, business continuity is no longer a project, but a continuing program that needs to be refined and evolved.

According to Ericson (2001), organizations need to create formal Business Continuity Management systems by applying Business Continuity Planning.

The Business Continuity Institute (BCI, 2007) defines Business Continuity Management as:

'A holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience with the capability for an effective response that safeguards the interests of key stakeholders, reputation, brand & value-creating activities.'

The Business Continuity Management Guide (2003) depicts Business Continuity Management as an umbrella activity integrating a wide range of business and

management disciplines, both in the private and public sectors, including crisis management, risk management and technology recovery, and should not be limited to disaster recovery in information technology (PAS, 2003).

Business Continuity is a system developed by professionals to minimize the impact of unforeseen events on the ability of the business to meet customer requirements (Zsidisin, Melynk & Ragatz, 2005). Elliott et al. (1999) stated that business continuity planning from the financial market side is a planning that defines the organization's exposure to internal and external threats and creates tough and gentle assets for effective prevention and recovery of the organization while preserving the competitive advantage and integrity of the organization.

Furthermore, Shaw and Harrald (2004) recognize that Business Continuity Planning is a key aspect of business continuity management, which contains business practices that offer focus and guidance on the decisions and actions required to prevent, mitigate, prepare, respond, and recover from a crisis. Business Continuity Planning includes the progress of a group of processes for the several business units that will guarantee the continuance of critical business processes although the data center is recovered from the disaster (Wilson, 2000). The BCP can also be defined as an integrated process of evolving measures and procedures to confirm the readiness of a disaster organization. This includes guaranteeing that the organization is able to respond effectively and effectively to a disaster and that critical business processes can continue as usual (Business Contingency Preparedness, 2002)

Banks are exposed to threating events, some of which may be serious and result in the failure to meet some or all of their business responsibilities. Events that destroy or inaccessible bank structure, communications or information technology or a pandemic affecting human resources can lead to significant financial losses to the bank as well as broader disruptions to the financial system. To provide flexibility against this risk, a bank will need to develop business continuity plans according to the nature, size and complexity of their business. These plans should take into account different types of possible or reasonable

scenarios in which the bank may be vulnerable (Basel Committee on Banking Supervision, 2011)

Moreover, continuity management should include business impact analysis, recovery strategies, testing, training and awareness programs and communication and crisis management programs. A bank should identify critical business activities, core internal and external addictions, and appropriate levels of resilience. Possible disruptive scenarios for their economic, operational and creditworthiness impact should be assessed and the resulting risk assessment should be the basis for recovery priorities and targets. Continuity plans should set out emergency strategies, recovery and repeat procedures and communication plans to inform executives, employees, regulators, customers, suppliers and, where appropriate, civilian authorities (Basel Committee on Banking Supervision, 2011)

Last, a bank should occasionally review its continuity plans to guarantee that emergency strategies are remain reliable with current operations, risks and threats, flexibility requirements and recovery priorities. Training and awareness programs need to be applied to permit staff to carry out effective contingency plans. Plans should be periodically checked to ensure that recovery targets and repetition and time frames can be met. A bank should also be involved in disaster recovery and business continuity testing with key service providers. The results of the official test activity should be reported to the management and the board (Basel Committee on Banking Supervision, 2011).

According to Herbane (et al 1997) banks should invest in Business Continuity Planning in order to create an organization and infrastructure, to ensure:

- Maintain the market position
- Maintain the trust of customers, governments, and shareholders - Keep good employees and customers
- Prevent liabilities towards employees, shareholders and customer claims
- Prevent losses in business.

Business Continuity Management is a successful business continuity planning that not only helps recovery but also ensures the continuity of operations and processes of key business strategies and revenue delivery units. It would also contribute to the continuation of bank administrative and banking support functions. The plan must include (MacSweeny, 2003):

- Prevention: Identify these measures and activities that reduce the possibility of inconsistency or accident occurring in the bank or in any of the delivery/support units.
- Response: When an event occurs there are some policies, procedures, and actions that should be followed by a continuation of work, mitigation, and security of staff, data and equipment.
- Resumption: The process of designing and implementing the repetition of only the most sensitive banking jobs immediately after a crash using an alternative site.
- Recovery: The process of designing and implementing the resumption of less sensitive banking operations directly after the cessation
- Restoration: Repair / Relocation of the original space and restoration of normal work.

Furthermore, the objectives of a good business Continuity Management according to MacSweeny (2003) are:

- Effectiveness
- Efficiency
- Easy to apply
- Good documentation
- Tested (frequent check)
- Flexibility
- Well reported
- Comprehensive - covering critical business operations

2.7.1. Operational Risk and Business Continuity Planning

The managing or the planning of the continuation of activities plays an important role to an organization. By developing, implement and maintenance of the frameworks, programs and policies helps the organization to manage a business event. Furthermore, imparts resilience to the organization by dealing with the likelihood and the consequences of the event. Therefore, it is important to have effective ORM and business continuity planning frameworks. Planning business continuity helps prevent, prepare, respond, manage, and recover from the effects of an incident or disorder (Storkey, 2011).

Every management framework includes five key elements. The first element, which is the same both business continuity planning and operational risk management, is to formulate the strategy, both business continuity planning and operational. The goal of this element is to minimize revenue instability by reducing risk. Business Continuity Planning and Operational risk management have key roles in this strategy.

The risk management process includes three main steps:

- Risk identification and evaluation;
- Treatment;
- Monitoring and assurance.

Business Continuity Planning starts with the impact analysis. Hoffman (2002) argued that 'Business continuity risk assessment is the most critical step. It requires an evaluation of the business line's inherent risk relative to revenue, reputation, a risk of one-time loss and regulatory requirements.' The impact analysis includes:

- A list of the activities required to implement basic services
- Assessment of the effects of the interruption;
- Calculation of the maximum allowable stoppage time
- Estimation of the minimum level of desirable service.

Operational risk manager plays an important role in the process of identification and evaluation. Therefore, operational risk manager because of his knowledge will be able to list the critical process, he may need to mitigate the risk by establishing more controls or to transfer the risk through various measures (Vaid. 2008).

One of the key features of operational risk is that if it is not adequately addressed, it may be spread and pose a threat to the continuity of the business. Therefore, it is important to define indicators for the continuous measurement and monitoring of the impact of an operational risk. These markers must have a tolerance limit so that once violated, the situation has to be seen as a matter of continuing business. According to Hoffman (2002), every business line will undertake its own ongoing business risk management process in line with business standards.

Operational risk managers identify key risk measure, the Key Risk Indicators (KRIs). The Operational Risk Manager should ensure that acceptable thresholds for key risk indicators have been set, taking into account the business impact analysis established for the business continuity planning. For example, the system shutdown, which is a risk, then the control should go back to the backup connection, then the Key Risk indicators should be the shutdown time. Financial institutions proceed with extensive self-assessments regarding audits for them. These will include key risk indicators for both operational risk and business continuity planning. Audits carried out at the facility will also cover all operational and business continuity planning risks and therefore provide assurance that the controls to mitigate these risks were at the highest level. These risks are therefore in the same continuous (Vaid. 2008).

2.7.1.1. Cyber Threats and Business Continuity Planning

A business continuity plan is vital for every business organization, and its main role is to assure the continuity of critical business operations and the fast recovery of key business activities in case of a crisis event occur. The successfulness of a business continuity plan depends on it should report all the

potential risks connected to main business operations which should be identified, assessed and efficiently planned for. Nowadays, information technologies become more risky for business organizations and communications with customers and suppliers, the cyber threats events are increasing as a result of leading to a disaster for business organizations. Organizations, in order to effectively deal with these events, should understand how cyber threats can affect their critical business activities. Hence, cyber risks should be considered as an important issue in business continuity planning. Business continuity planning is linked to the development, implementation and regular update of frameworks, programs, and policies aimed primarily at avoiding potential business turbulences caused by expected or unexpected events. An important part of business continuity planning is to conduct risk analysis and business impact analysis to identify possible threats that could cause business disruption. Moreover, Business Continuity planning is directly connected with organization's risk management planning.

The risk to Cyber Security is defined as a risk to information and technology that have as consequences to affect the availability, integrity, and confidentiality of information or information systems and can be separated into four categories: technological failures, failed internal processes and external events (Cebula J and Young A, 2010). Cyber risk contains a group of risks is not a specific risk but it is presented as a group of risks and can be differentiated based on technology, means, and direction of the attack and have a possibly great impact on the target. The effect can be both legal liability and computer security breaches to privacy breaches or theft of confidential data (Barzilay, 2013).

The Bank of England's Systemic Risk, in 2013 published a survey where was reported that there is an increase of 10% regarding operational risk, further, the most mentioned risk to this survey was the threat of 'cyber' attacks. According to a survey developed in 2015 from Price Water House Coopers based on the Global State of Information survey, the number of information security events has increased from 28.9 million in 2013 to 42.8 million in 2014 (a 48% increase). The results of these incidents are that are costly and damage the organization's

reputation. Due to the fact that the cyber risk incidents are increasing dramatically, the Federal Financial Institutions Examination Council (FFIEC) has reviewed their Business Continuity Planning guidelines for the financial services sector, with including to this new version a planning to support cyber-resilience. In this new version was included a list with specific cyber risks such as malware, insider threats, destruction and corruption of data or systems, and communications infrastructure disruptions such as Denial of Service (DDoS) attacks.

The meaning of Cybersecurity risk management is that business organizations need to pay more attention to cybersecurity. Cyber risk concerns all those directly involved in an organization, thus it should attract the attention of senior executives and the board of directors (Dunbar, 2012).

A business continuity plan for the timely recovery of critical business-to-business needs to be set up, tested and implemented. Throughout the business continuation process, information security must be woven as an integral part of it. Business continuity planning should meet the requirements of information security and must comply with them as any other procedure in the organization should. Business continuity recovery is a key information security area for the next 12 months (Global Information Security Survey, 2013). Moreover, the main goal of business continuity planning is to an organization to return to business as usual operations as soon as possible and this is the reason that an organization should have to implement a business continuity planning during a cyber threat event.

An effective plan starts with the senior management and the board, who are responsible for risk management and control. The effectiveness of the plan depends on the willingness of the administration to commit itself to the process from start to finish. By working as a member of the implementation team, it can ensure that both the audit committee and the senior management understand this commitment and realize that shutting down the business from cyber-attacks is a high risk to the organization that deserves high-level attention. The purpose

of this analysis is to determine the impact of cyber threats and related events on all business processes of the organization. The assessment for all operations, processes, and staff, including specialized equipment requirements, external relations, alternative job requirements, staff training and staff support, such as specialized training and human resources guidance on related personnel issues, is very critical for the organization.

Therefore, in the phase of risk assessment of the business continuity planning process, an organization should also proceed with the assessment of cyber risk. This will process include the identification and address of the cyber challenges, thus, organizations should analyze and understand the connection between their business operations and the cyberspace. It is important to identify key elements of cyberspace and what basic business functions and mission abilities support. This guarantees the achievement of cyber resistance and helps assess the impact of loss due to a particular cyber-space.

In business continuity planning, by including the cyber risk, contributes to testing the performance and capabilities of cyber assets and also assumes that there may be weaknesses in cyber-related businesses that could be referred to as domains improvement. The business continuity plan is incomplete if it does not take into account the need for preserving the availability of mission which is a critical cyber element. Thus, continuity planning for the cyber threat is a continuous process for all organizations that must remain flexible as they change and migrate daily threats (Britton C., 2017)

2.7.1.2. External Fraud and Business Continuity Planning

Fraud is one of the most negative factors in society and because of fraud, some companies face many financial problems and even business continuity problems. In the current environment, high technology and information systems, not only the number of executed frauds has increased but also their volume (Mackevicius, Bartaska, 2003; Mackevicius, 2012). The globalization, the financial flows, and markets, Internet use, mergers and divisions of companies, the increasing competition, political and economic factors are factors which contribute, a fraud

incident to occur (Lakis, 2008, Mackevicius, 2012).The Identification of fraud is not easy and requires detailed and specific knowledge about the company's economic activity, a possibility of the existence of fraud and their characteristic.

Fraud and financial outcomes for businesses are a disaster. In Finance sectors, business continuity is relevant for business management because fraud continues to spread throughout the world (ACFE report, 2012). Business Continuity Planning (BCP) allows organizations to move forward and survive through various catastrophic circumstances or events. Business Continuity planning and disaster recovery should be addressed primarily through a well-prepared 'Emergency and Disaster Recovery Plan'(O'Hehir, 2007). There are many and possible catastrophic circumstances or events, we are focusing on potential Fraud is one of the possible catastrophic and disaster events that organization can cope, thus, is important to focus how best to reduce the opportunities for fraud. According to O'Hehir (2007), if managers do not monitor the environmental management and internal control issues are likely to increase opportunities for fraud. Therefore, to reduce opportunities for financial fraud and, by extension, financial cost, management at all levels requires timely, current and relevant financial details.

According to O'Hehir (2007), there are four areas connected and related to justifying the opportunity for operational, economic and disclosure of fraud: environment, asset management, fraud and financial control. Fraud is directly linked to the business risk approach to managing the business continuity in the face of a disaster.

Moreover, fraud is an ever-increasing barrier to risk management and business continuity. In addition, frauds are not always disclosed or reported, and so it’s difficult to identify the exact nature of all the adversities arising from fraudulent activities. Business continuity requires an organization to undertake dynamic efforts in an ever-changing business environment. Undoubtedly, these efforts may worsen in the face of fraud. Thus, fraud risk management becomes

imperative for active risk management to reduce the likelihood of fraud occurring during the business continuity planning process (O'Hehir, 2007).

The framework of business continuity planning consist to help BCM provides a framework to guide the organizations and their management to identify, avoid and respond to business risks. O' Hehir (2007)argued that a business continuity plan must be up to date and to reflect the current business environment, should allow changes in the business environment and procedures should be in place to ensure that it is kept up to date. Similarly, internal controls should be adapted to cover changes in the business entity and the changing environment. Concerning the continuity of the business, enterprise risk management is focusing on fraud issues with an enterprise-wide perspective (Von Rössing 2007). Enterprise risk management is stepping up its work as it seeks to include all relevant actors in the organization's active risk management model. Business Continuity Management supports a practical approach to risk management across the organization. It focuses on identifying and managing assets that are critical to the effective operation of the business.

2.8. Risk Assessment

A risk assessment process is a tool which used to provide with information the decision makers for understanding the factors that can harm and impact operations and products, and express concern about the level of action required to reduce the risk. The identification of the risk, the estimating possibility, the estimation of potential losses and damage and the identification of the cost-effective process are action taken during the Risk Assessment process (U.S. GAO 1999).

Furthermore, Risk assessment is one of the critical steps of the risk management. Risk Assessment can be used to create appropriate policies and select techniques to implement them. Because of the changes of the environment, the risks are changing too, thus, is very important for an organization to assess the risks occasionally, and update and adjust the policies and controls, if needed, in order to effectively handle the risks (U.S. GAO 1999; Stoneburner et al 2002).

Regarding, Dong and Copper (2016), risk assessments are beneficial for businesses to gain the necessary information to identify factors that have a negative impact on businesses and products, which helps them make better decision-making and design better countermeasures to reduce risks. With assessing risk, organizations can ensure that decision makers can focus on the most important risks and threats and prepare the organization to deal with the risks. In addition, the impact of each risk and the overall risks should be taken into account and all risks should be reviewed regularly (Liu et al., 2017). The risk assessment also addresses the prioritization of risk levels. Ritchie and Zsidisin (2008) emphasized that the risk assessment process involves quantifying risks, assessing possible consequences and the level of risk impact. Risks have various types, with different nature, they appear in different time and size, so = the different types of risks have different evaluation methodologies and it depends on the organization's management to choose the right method of estimation.

There are several models for risk assessment. The range of risk assessment determines the extent of the analysis and resources. Risk assessment quality depends on the availability of the data. The assessment process requires data on the probability of risk, the cost of the damage and the risk mitigation cost to determine the monetary cost of the risk in the quantitative approach. however, the lack of data such as risk probability and loss of impact, a qualitative approach will be applied to risk assessment by risk identification with a more subjective and general term such as low, medium and high. In some cases, analyst combines the two approaches to the semi-quantitative approach in some cases (U.S. GAO 1999). Risk assessment is based on the development of evaluation criteria, the evaluation of risk interactions and the risk hierarchy (Cooper et al, 2005). The development of assessment criteria can be done by developing probability and impact for risk assessment and has two-dimensional.

Assessment of risk interactions: any risk is not individual, a risk may interact with other risks to see how each risk affects one another.

Prioritizing risks: the process of identifying risk management priorities, identifying significant risks that are highly likely and high impact. The goal of risk assessment is to adopt the business strategy to provide an opportunity to reduce risks. According to Cooper (2005), the qualitative analysis is based on descriptive scales such as low, medium and high for the description of the probabilities and the impact of the risk. When the organization needs to make the quick assessment and initial review, this approach must use. Aqlan et al., (2015) stated that risk assessment plan including risk modeling and impact measurement

On the other hand, the Quantitative analysis uses numerical odds ranges for the probabilities and the impact instead of description ranges (Cooper, 2005). Quantitative analysis includes the assigning priority (Aqlan, Lam, 2015 and Cooper et al., 2005).

Cooper (2005) has proposed a third approach for risk assessment the Semi-quantitative, which is a combination of the Qualitative and Quantitative analysis.

2.8.1 Cyber Threats and Risk Assessment

There are two main things that distinguish the risk assessment within cyber threats from the general operational risks. Firstly, the cyber threat is widespread, global. Secondly, the number of possible sources and threats, both malicious and non-malicious, is too great. In combination, this means that the search area and the number of sources of potentially relevant information on cyber-risk are extremely large and may seem overwhelming. The risk assessment step is divided into two separate steps: The first step focuses on malicious cyber-business risks and the second step is focusing on non-malware cyber threats. The identification the threat depends on the nature of threats, the vulnerabilities, and if it's a malicious incident or not.

The first step has a goal to identify the risks based on the possible ways that cyber risk occurs. It is very important to identify the motivations, intentions, abilities, skills, resources. Furthermore, by identifying cyber risks that were

caused by malicious threat, a manager needs to identify potential sources of threat too. In general, the first step is to identify the cyber threats and the sources of these threats. In conducting the second step of risk assessment, you need to clarify what can go wrong in order to have efficient and effective results in dealing with the threat.

Federal Financial Institutions Examination Council (FFIEC), in 2014 piloted a cybersecurity assessment at over 500 community financial institutions to evaluate their disaster recovery preparedness to mitigate cyber risks. The results from this Cyber Security Assessment was to find out the range of risks inherent in financial institutions and it also suggested actions to be taken into account by management and board members when assessing cybersecurity and the readiness of their financial institutions (Kitten, 2015).

It is important for management to understand the inherent risks of the financial institution cyber threats and vulnerabilities in the assessment of cyber-disaster recovery preparedness (Kirvan, 2011). Therefore, after the completion of the development of a standard risk and cyber assessment, managers can proceed with the development of disaster recovery strategies (Kirvan, 2011).

2.8.2. External Fraud and Risk Assessment

The term Fraud is a social phenomenon and each fraud has different characteristics depending on the type of industry (Francis, 2013). Any organizations are vulnerable to fraud. Undoubtedly, the fraud risk assessment is critical to auditors, and this is supported by the standard that requires auditors to have professional skepticism when performing control (International Standard 240). The auditor also performs a fraud risk assessment and financial statement audit, which may affect the fraud risk assessment performance (Braun, 2000; Knapp & Knapp, 2001). The failure to identify the risk of fraud can raise concerns about the auditors' responsibility for fraud risk assessment (Chen, Kelly, & Salterio, 2012). Therefore, auditors should carry out a fraud risk assessment, which includes the judgment of the auditors to assess the presence of the risk of fraud in an organization. Auditors should maintain a high risk-of-

fraud rating, as the poor performance of the fraud risk assessment would lead to loss of income and a crisis of trust among the public. Auditors need to understand the characteristic of the activity involved in the execution of the fraud risk assessment process (Duh, Chang, & Chen, 2006).

The use of Standards and guidelines encouraged the implementation of the exchange of ideas during the fraud risk assessment. Studies have shown that the exchange of ideas can help auditors improve the quality of control. Additionally, although the structure and structure of the work may affect the risk of fraud, there is a lack of data on the interaction between the exchange of ideas and the structure of work on the performance of fraud risk assessment.

Moreover, the risk assessment of fraud has been defined as an assessment of potential fraud affecting the organization's ability to maintain its functions and reputation (Association of Certified Fraud Examiners, 2016). Assessing the risk of fraud should also identify and address the vulnerability of an organization to internal and external fraud. Senior managers and board of directors should take the initiative to carry out a fraud risk assessment in their respective jurisdictions. While the international standard of auditing requires auditors to identify and evaluate the risks due to fraud. Hence, auditors must continuously carry out a fraud risk assessment as it is a continuous process. Auditors should carry out a fraud risk assessment during commitment, audit planning, on-site inspection and final control (Payne & Ramsay, 2005). The guidelines suggest that the brainstorming method is used as a tool to improve the risk of fraud risk and to overwhelm the failings of a similar practice. In addition, there is a variety of the structure of tasks in assessing the risk of fraud.

Blank Page

Chapter 3
Research Methodology

3.1. Introduction

This research was conducted to examine integrated presentation in one of the most popular risk where international banking sector should tackle daily. We will focus on two categories of Operational Risk, Cyber Threats and External Fraud, and related factors as well as how they affect business continuity of international banking industry. This study would help other researchers to demonstrate the theory and support the future research, produces good ideas and delivers better understanding. Moreover, this study aims to provide a practical guidance on best practice regarding an effective way of operational risk assessment in banking sector. It will further contribute to build knowledge on methods used to assess operational risks, the area of operational risk assessment, provide suggestions to the improvement of the operational risk assessment in the banking system.

To examine these research goals, the researcher decided to use a combination of qualitative and quantitative research methods, including develop a questionnaire which administered to Bank Employees and interview schedule used to collect information on the Operational Risk, External Fraud and Cyber Threats and a questionnaire, which was been answered from bank employees. Simple Random Sampling used to administer the questionnaires to ensure statistical conformance. Data collected was analyzed qualitatively and quantitatively, using SPSS as well as Microsoft Excel.

3.2. Research Design

The descriptive method of research was used for this study. According, to, Creswell (1994), the descriptive method of research is to collect information

about the present existing condition. The purpose of descriptive research is to prove formulated hypotheses that refer to the present situation in order to clarify it. The descriptive method is quick and practical in terms of the financial aspect. Furthermore, this method it gives you the opportunity and flexibility when important new issues and questions arise during the study, further investigation may be conducted.

3.3. Primary Data

In this study, the descriptive research method was engaged so as to review operational risk management process to the banking system and to classify the impact of risk assessment and also the effect of business continuity. The researcher decided to use this research method considering the objective to obtain first hand data from the respondents. This method can use either qualitative or quantitative data or both, giving the researcher more alternatives in selecting the instrument for data-gathering.

The research is using bank employees as respondents from public banks within the International Banking Sector, in order to gather relevant data. The descriptive method is then suitable as this can allow the identification of the similarities and differences of the respondents' answers. The Primary data is data which has not been collected from previous research. Such data is gathered firstly for the existing study. Primary data means the researcher gets information directly from the organization (Money, et al., 2000). The source of primary data comprises research, observations, surveys and interviews, focus group discussions, case study. Primary data is collected for the specific research by using google doc's tool, which is also its main advantage. It can make the research reliable and objective. (Ghauri, Grönhaug, 2002)

Statistical tool used to understand such data. Therefore, the technique is perfect and results in careful findings. Nevertheless, collecting such data is time consuming and difficult. Respondents act as sources for primary data when the incidents occur. Data is collected through interviews and reports. Reports may

also be gathered from individual interaction journals (Singleton and Straits, 2005).

3.3.1. Case Study

The qualitative approach to research is used to answer questions about the nature of phenomena with the purpose of describing and understanding them from the participants' point of view. Case studies are a form of qualitative research, which are defined by interest in individual cases. This study is to find out the situation and suggestion in performance appraisal of bank employees. As a result, a case study approach is suitable in this work. There are several definitions and understandings of the case study. Bromley (1990) defined the case study as a systematic investigation into an event or a set of related events which has as purposes to describe and explain the phenomenon of interest.

A case study means that the qualitative method is used (George, Bennett, 2005), and it is about the "real life context" (Yin, 2003). Specifically, Yin (2003) said that case study is that investigating the phenomenon from the reality. The case study not only requires that evidence and data collections must come from the reality, but also needs a complete observation on the research. Therefore, case studies apply a useful and effective method in management research, especially when investigating "Why" and "How" question (Blumberg et al, 2005).

Furthermore, Case studies are used when the researcher aims to support his argument by an in-depth analysis of a person, a group of persons, an organization or a project. The case study approach is not limited in value, it offers an in-depth analysis of a specific problem. Naoum (1998), and Gall, Borg, & Gall (1997) categorized case study design into three groups. The Gallo and Horton study (1994), shows a descriptive case study, Kos's (1991) research provides an example of an explanatory case study, and an evaluative case study is showed by Butler's (1995) work. Yin (2003) identified at least six kinds of case studies.

A Case study research can be based on single- or multiple-case studies, whether single or multiple, the case study can be exploratory descriptive, or explanatory. A single case study focuses on a single case only, while a multiple case study may include two or more cases in the same study. An exploratory case is intended at defining the questions and hypotheses of a study or at determining the viability of the desired research procedures. A descriptive case study presents a complete description of a phenomenon within its context. An explanatory case study offer data about a cause-effect relationship, explaining how events happened. Almost any phenomenon can be examined with a case study method. While some researcher's emphasis on the study of one case because of its unique qualities, other researchers study multiple cases to make comparisons, build theory, and propose generalizations. This survey is a case study about the performance appraisal of Hellenic's Bank employees.

To classify the factors connected with Operational Risk of cyber threats and External fraud in International Banking Industry and the influence of cyber threat and external fraud for a crisis in the banking industry with malfunction at the business continuity planning, a total of 102 respondents were asked to participate. The participants qualified for sample selection must be employees of a bank.

For the sample selection was used a Simple random sampling. This sampling method is conducted where each member of a population has an equal chance to become part of the sample. As all members of the population have an equal opportunity of becoming a research participant, this is said to be the most effective sampling procedure.

Quantitative data collection methods are focused on the quantification of relationships between variables. Quantitative data-gathering instruments found relationship between measured variables. Measurement, numerical data and statistics are the main material of quantitative instruments. With these instruments, a clear description of data collection and analysis of procedures are

necessary. The quantitative method is describing a phenomenon with more details. Basically, gives a generalization of the gathered data.

Quantitative method it helps the researcher to prevent bias in gathering and presenting research data. The quantitative data collecting methods are useful when a study needs to measure the cause and effect relationships evident between pre-selected and discrete variables. The purpose of the quantitative approach is to avoid subjectivity by means of collecting and exploring information.

Quantitative methods establish very specific research problem and terms. For the Quantitative method, are needed both variables, dependent and independent, which must be clearly and just specified in a quantitative study. Fryer (1991) mentioned that qualitative researchers aim to decode, describe, analyze and understand the meaning of a certain phenomenon happening.

On the other hand, qualitative approach generates verbal information rather than numerical values (Polgar & Thomas, 1995). Instead of using statistical analysis, the qualitative method uses content or holistic analysis. The aim of the quantitative research method is that measurement is valid, reliable and can be generalized with its clear expectation of cause and effect (Cassell & Symon, 1994).

3.4. Instruments

The survey questionnaire was used as the main data-gathering instrument for this study. The researcher developed a questionnaire, including questions about the operational risk, cyber threat and fraud, risk assessment, business continuity planning as well as several demographic questions such as age, the number of years as they are working in the organization and their job position.

For this survey, the type of the question used was structured, mixed structured and semi-structured questions. Questionnaires were administered to different banks and departments of the banks. Furthermore, interview schedule was also

used to get more information about the operational risk management and the importance of the business continuity planning in banks and to examine the importance of the operational risk assessment. Different types of questions were used to extract the needed information from employees of the Bank, Structured Questions which inquiries that can be answered only in a specific way, such as totally, not at all, to a fair degree, to a smaller degree, not at all, yes/ no, strongly agree, disagree, neutral, agree, strongly disagree. These were used to collect information from respondents in a way that did not give them the opportunity to express their opinion in their own words. These were used generally to extract employees' views on the subject. Semi-structured questions are those whose fillings are not fully specified in advance. Respondents are encouraged to provide answers in their own words, to support their opinion and their feelings. Often the information obtained from semi-structured interviews will provide not just answers, but the reasons for the answers and hence its acceptance in the study. Last the Semi-structured interviews mix structured questions with open-ended questions that ask why and how. Open-ended questions were used to follow up and investigation for more detailed and explanatory answers. The structured questions in semi-structured interviews were quantified. Open-ended questions were more difficult to administer because follow-up questions should be asked in a uniform way for each respondent.

3.5. Secondary Data

Secondary data analysis is any further analysis of an existing dataset which offerings interpretations, conclusions or additional or different knowledge from those produced in the first report on research and its main results. (Hakim, 1982)

In this study, the secondary data that was used was from books, articles, organization studies and another published.

3.6. Data Processing and Analysis

For analyzing data we used qualitative and quantitative techniques. By using content analysis and logical analysis we succeeded to describe the patterns in the data. Primary data obtained from questionnaire administered to employees of different Banks and was analyzed with SPSS. The SPSS software helped to analysis the first data that was collected from the questionnaires into simpler quantitative and tables form for easy understanding and assimilation. In addition to SPSS, Microsoft Excel was used to generate the diagrams from table's obtained.

3.7. Validity and Reliability

Marshall and Rossman (2006) argued that any inquiry in the qualitative paradigm must face the conditions of applicability, consistency and neutrality, like, internal and external validity and reliability. Lincoln and Guba (1985) modified the terminology for the interpretive of qualitative research. The proposed constructs are credibility, transferability, dependability and conformability. These alternative methods have been suggested as suitable to ensure validity and reliability in a qualitative research. (Babbie& Mouton, 200, Marshall & Rossman, 2006, Whittemore, Chase & Mandle, 2001).

- Credibility. The aim of credibility is to ensure that the subject is suitably identified and described. By the appropriate definitions, limits and restrictions on the methodology followed in the study, its credibility will be enhanced (Babbie& Mouton, 2001, Marshall &Rossman, 2006, Whittemore et al., 2001).
- Transferability. This refers to the generalization and usefulness of the results in similar situations. In qualitative research this aspect is problematic, but overcoming this can be achieved by referring to the original theoretical framework where mention how data collection and analysis is directed by concepts and models (Marshall & Rossman, 2006). Strategies to enhance transferability include providing thick descriptions of data and the use of direct sampling (Babbie & Mouton, 2001).

- Dependability. This term is referred to the attempts which were made by the researcher take into account for changing conditions in the phenomenon selected for study, as well as changes in design. This assumption is based on the idea that in qualitative research the social world is always being constructed, thereby making replication difficult (Marshall &Rossman, 2006). Guba and Lincoln (1985) recommend a single properly managed control to determine dependability and confirm ability.
- Confirm ability. The question asked here is whether another researcher could confirm the findings of the research, that is, do the interpretations meaningful and can the logic and findings be made transparent to others (Marshall & Rossman, 2006). Confirm ability is about the degree to which the research findings are a product of the inquiry and not the biases of the researcher (Babbie & Mouton, 2001). As previously mentioned, an audit trail should be left to enable the researcher to identify if conclusions, interpretations and suggestions can be identified to their sources (Babbie& Mouton, 2001).

	Actions taking by researcher
Credibility	• Adoption of appropriate, well recognized research methods • Random sampling • Use of different methods, different types of informants and different sites • Examination of previous research to framework findings
Transferability	• Study previous data in order to establish context of study and detailed description of phenomena to the questions of the questionnaire to allow comparisons to be made

Dependability.	• In-depth methodological description to allow study to be repeated • Use of individual interviews • The research design and its execution, describing what was planned and executed on a strategic level
Confirmability	• In-depth methodological description to allow integrity of research results • Use of diagrams

Table 1. Methods suitable to ensure validity and reliability in a qualitative research

3.8. Flow Diagram

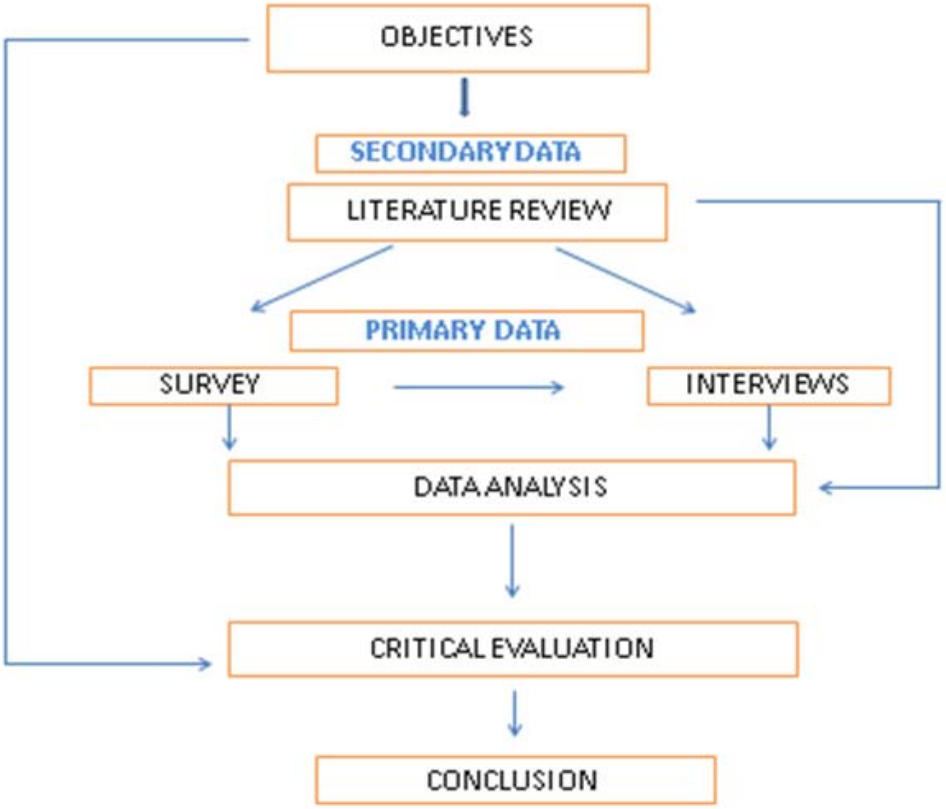

Figure 1. Flow Diagram

Chapter 4
Data Analysis and Discussion

In this chapter, the results of this research are presented and, an analysis and evaluation of the findings, both qualitative and quantitative. The first part is a qualitative method, with the analysis of the questionnaire. The second part is the quantitative method, with analysis of the interviews. To address the research questions, a correlation coefficient analyses were interpreted and discussed to review the factors connected with operational risk of Cyber Threats and External Fraud in Banking industry, to classify the impact of Cyber Threats and External Fraud as factors for a crisis in the banking industry with malfunction at the business continuity planning and the importance of operational risk assessment in the banking sector.

The questionnaire for this survey was been answered by 103 bank employees.

Having in mind the basic results of the statistical analysis and for further analysis was made 5 interviews from 1 manager, 1 sub – department manager, 2 supervisors, and 1customer support officer, in the banking division.

4.1. Operational Risk, Cyber Threats and External Fraud in Banking Division

4.1.1. Operational Risk in Banking Division

In the middle of 1990s a new risk appeared in the business division, the Operational Risk. This type of risk was existed and before but it was not interpreted until after 1995 when Barings bank, one of the oldest banks in London, collapsed because of Nick Leeson, one of the traders, due to unauthorized speculations(Moosa,2008).

Operational risk has variety of definitions, one of the most integrated definition of Operational risk is the one of Basel II Committee. According to The Basel II Committee, operational risk can be defined as the risk of loss because of poor or failed internal processes, people and systems, or from external events (Basel Committee on Banking Supervision, 2001). Moreover, losses due to an IT failure, transactions errors, external events like an earthquake, or a fire such as the one at Crédit Lyonnais in May 1996 which has as a result in extreme losses, are some examples of operational risk.

The last decades, operational risk is one of the most crucial risk in the banking industry due to the increased complexity and globalization of the financial system, the expansion of the internet and the rise of social media, as well as the increasing demands for greater corporate accountability worldwide and the recent appearance of extraordinary large losses. In October 2014, the Basel Committee decided to propose a revision on operational risk framework. In this proposal included new aspects of operational risk such as privacy protection, legal risks, physical or environmental risks fraud, and security (Basel Committee on Banking Supervision, 2014).

Furthermore, Basel II includes seven types of Operational Risk (Basel Committee on Banking Supervision, 2011):

- Execution, Delivery, and Process Management – data entry errors, accounting errors, failed mandatory reporting, negligent loss of client assets
- Business Disruption and Systems Failures – utility disruptions, software failures, hardware failures
- Damage to Physical Assets – natural disasters, terrorism, vandalism
- Clients, Products, and Business Practice – market manipulation, antitrust, improper trade, product defects, fiduciary breaches, account churning
- Employment Practices and Workplace Safety – discrimination, workers compensation, employee health and safety

- Internal Fraud – misappropriation of assets, tax evasion, intentional mismarking of positions
- External Fraud – theft of information, hacking damage, third-party theft and forgery

4.1.2. External Fraud in Banking Sector

A phenomenon of the Operational risk the banking sector is Fraud. Fraud contains a wide range of illegal practices. The Institute of Internal Auditors' "International Professional Practices Framework (IPPF) defines fraud as: "Any illegal act characterized by deceit, concealment, or violation of trust. These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by parties and organizations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage."

Furthermore, when a bank faced a fraudulent incident this has an impact to the organization in several areas including financial, operational, and psychological. Loose of reputation, customer relations are reasons that a bank can been driven to disaster.

The U.S financial institution, based on KMPG records (2011), has discovered fraud case involving a complex loan application which was affected by the senior manager to operate non-performing loans into performing loans. According to Association of Certified Fraud Examiners (ACFE) (2014) 36.6% happens in the banking and financial services, government and public administration, and manufacturing fraud incidences where the highest percentage of fraud cases is in the banking and financial services (17.8%), with a median loss of $200,000 (ACFE, 2014).

A type of fraud is the External Fraud which is defined as unexpected financial, material or reputational loss as the result of fraudulent action of person's external to the organization. According to Basel II, external fraud are loses because of defraud, misappropriate property or circumvent the law, by a third

party. External fraud incidents differ by the number of people involved and the mechanism of attack. External Fraud events can be categorizing as below:

- Corporate Finance: Loan Fraud, Client Misrepresentation of Information, Theft
- Trading and Sales: Cybercrime, Forgery
- Retail Banking: Cybercrime, Check Fraud, Theft of Information, Theft of Assets
- Commercial Banking: Fraudulent Transfer of Funds, Credit Product Fraud (loans, letters of credit, guarantees)
- Payment & Settlement: Payment Fraud
- Mitigation

Strong internal controls which includes both of systems and processes and supported by the firm's risk culture embedded in employees, can mitigate the external fraud.

4.1.3. Cyber Threats in Banking Sector

Cyber threats phenomenon begins from 1975 when Steve Jobs and Steve Wozniak invented the first personal computer, the Apple I. A cyber threat can be defined as any malicious act that attempts to gain access to a computer network without authorization or permission from the owners. The last few years the cyber threats events have increase dramatically in the global banking division.

Nowadays, more and more customers using the digital channels such as internet banking, digital wallets, mobile banking, ATM. Therefore, the exposure is increasing and thereby cyber-attacks, which leads to financial, reputational losses, and lose of customer's confidence.

In 2016, Price Water House Coopers conducted a survey for Global Economic Crime, the result from this survey were that cyber-crime the second most reported crime globally and that 54% of organizations have been attacked with

cyber-crime. Banks are the main targets for cyber-crime. It is a fact that banks from all over the world have been hit by hackers, for example:

- Attacks against Tesco bank, where hackers stole over £2 million from customer accounts,
- DDoS attacks bring banks like HSBC to a standstill,
- Phishing scams targeting the customers of all major banks
- Malicious, careless and compromised users.

4.2. Demographic Characteristics

This section deals with section A of the questionnaire which is about the demographic characteristics of the respondent

4.2.1. Gender and Age

The first question was about how old is the respondent. Forty-one respondents were between 26 – 35 years old (39.8%), twenty-four were between 36 – 45 years old (23.3%), thirteen were between 56 – 59 years old (12.6%), twelve were between 46 – 55 years old (11.7%), twelve were between 18 – 25 years old (11.7%) and 1 was above 60(1%) indicated as shown in Figure

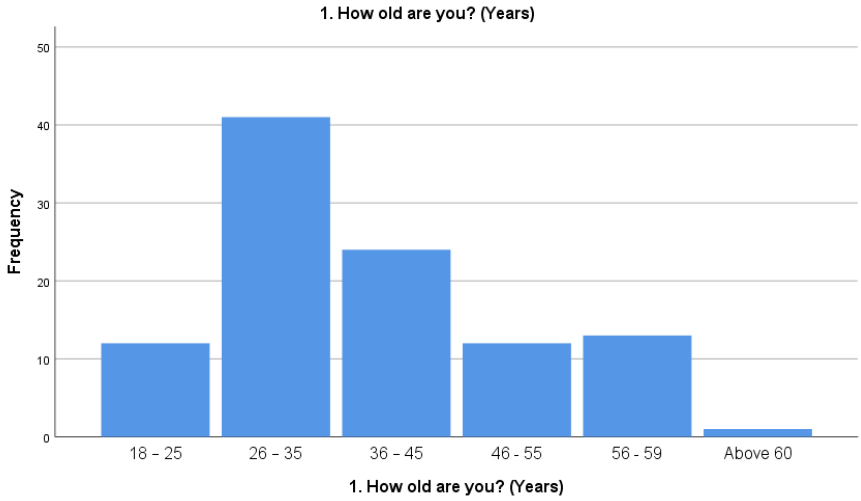

Figure 2. Age

The second question was about the gender of the respondent. Fifty-four respondents (52.4%) were Female and forty-nine respondents (47.6%) were male indicated as shown in Figure 4.1.

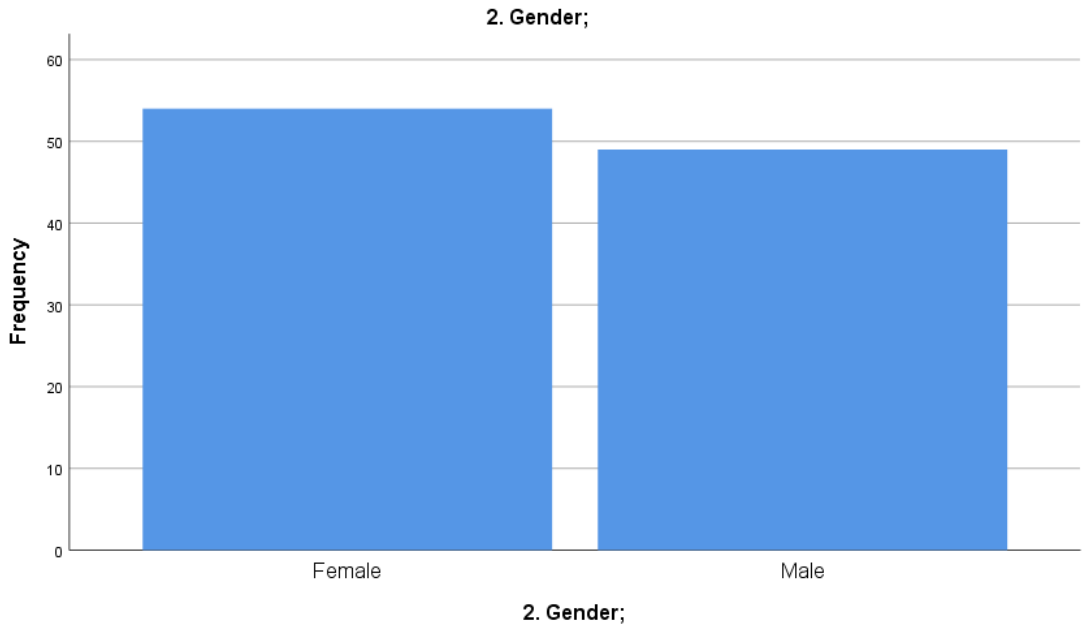

Figure 3. Gender

4.2.2. Educational Background

As figure indicated the level of education of the sample, 44 of them have master degree (42.7%), 39 first degree (37.9%) ,14 Professional degree(13.6%),3 senior high school degree(2.9%), 2 Doctorate Degree (1.9%) and other which is college degree (6.7%), and one Secretarial studies (1%).

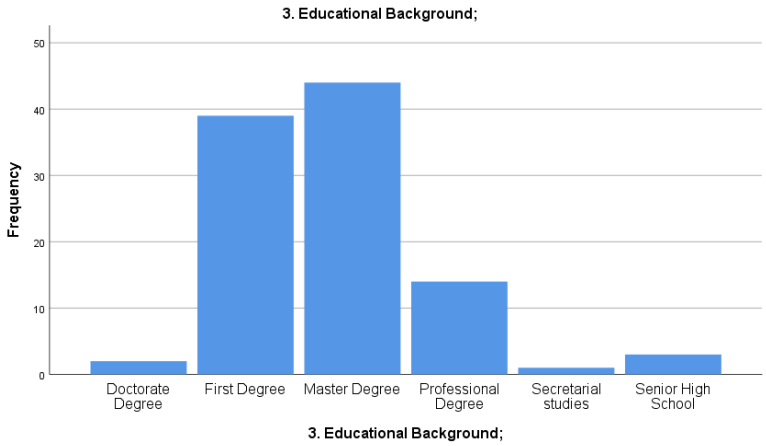

Figure 4. Educational Background

4.2.3. Job Position

The Fourth question was about the job Position of the repondent. Fifty - four the of the respondents work as Officers (52.9%), thirty - two as Supervisors (31.4%), fourteen as Managers (13.7%) and 2 as General Managers (2%).

Figure 5. Work Position

4.2.4. Working Years

The fifth question focused on the number of years the respondent working in the bank. Most of the sample is working to bank for 6 – 9 years (22.3%). 20.4 % of

the sample is working to the bank for 15 -19 years,19.4% of the sample is working for 1-5years,11.7 % is working 20- 24 years ,7 people are working for more than 25 years(6.8%) and 2 less than a year(1.9%).

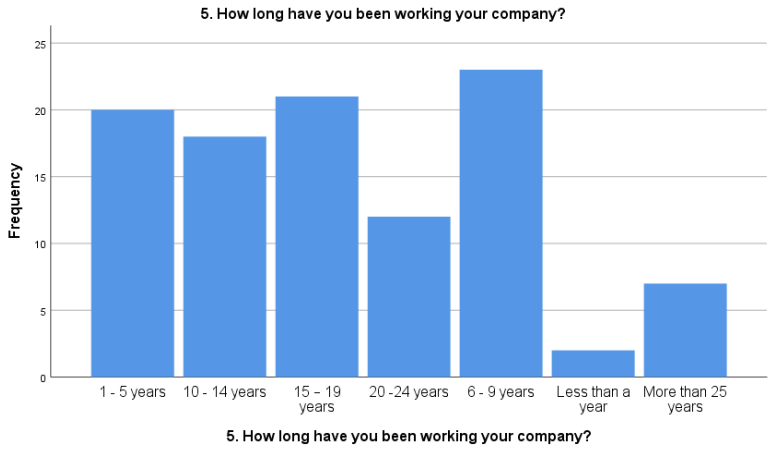

Figure 6. Years working in the company

4.3. Operational Risk in the Banking Sector.

The section B of the questionnaire explores the Operational Risk in Banking Sector

4.3.1. Primary operational risk types in Banking Sector

The first question was about which operational risks of banking sectors, the respondents classify as primary. In this question, as illustrated from the tables, most of the banks employees considered Cyber Risk, External Fraud and Regulations as primary Operational Types. According to the Risk. Net in the rank of the top 10 operational risks for 2017, Cyber Risk is in the first place, Regulations on the second and Fraud in the ninth place (2017, January 23).

To what degree would you rate the following as primary operational risk types within your organization? [Cyber Risk]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2= to a smaller degree	2	1.9	1.9	1.9
	3=to a fair degree	9	8.7	8.7	10.7
	4=to a high degree	33	32.0	32.0	42.7
	5=totally	59	57.3	57.3	100.0
	Total	103	100.0	100.0	

Table 2. Operational Risk Types

To what degree would you rate the following as primary operational risk types within your organization? [Regulation]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1= not at all	2	1.9	1.9	1.9
	2= to a smaller degree	3	2.9	2.9	4.9
	3=to a fair degree	12	11.7	11.7	16.5
	4=to a high degree	80	77.7	77.7	94.2
	5=totally	6	5.8	5.8	100.0
	Total	103	100.0	100.0	

Table 3. Regulation

To what degree would you rate the following as primary operational risk types within your organization? [Geopolitical]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1= not at all	60	58.3	58.3	58.3
	2= to a smaller degree	26	25.2	25.2	83.5

	3=to a fair degree	15	14.6	14.6	98.1
	4=to a high degree	2	1.9	1.9	100.0
	Total	103	100.0	100.0	

Table 4. Geopolitical

To what degree would you rate the following as primary operational risk types within your organization? [Physical Attack]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1= not at all	58	56.3	56.3	56.3
	2= to a smaller degree	29	28.2	28.2	84.5
	3=to a fair degree	6	5.8	5.8	90.3
	4=to a high degree	6	5.8	5.8	96.1
	5=totally	4	3.9	3.9	100.0
	Total	103	100.0	100.0	

Table 5. Physical Attack

To what degree would you rate the following as primary operational risk types within your organization? [Fraud]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2= to a smaller degree	1	1.0	1.0	1.0
	3=to a fair degree	8	7.8	7.8	8.7
	4=to a high degree	41	39.8	39.8	48.5
	5=totally	53	51.5	51.5	100.0
	Total	103	100.0	100.0	

Table 6. Fraud

4.3.2. Implement Primary factors of Operational Risk

The primary risk factors of operational risk were identified as people, processes, systems and external events in the literature study. The response concerning

how important banks regard these primary operational factors. According the definition of European Commission's Directive (2006): "Operational risk means the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events."

People: 65% of the respondents indicated that people is implemented as primary factor on operational risk in a high degree.

To what degree has your organization implemented the following primary factors of operational risk? [People]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2= to a smaller degree	3	2.9	2.9	2.9
	3=to a fair degree	21	20.4	20.4	23.3
	4=to a high degree	67	65.0	65.0	88.3
	5=totally	12	11.7	11.7	100.0
	Total	103	100.0	100.0	

Table 7. People

Processes: 58.3% of the respondents indicated that processes is implemented as primary factor on operational risk in a high degree

To what degree has your organization implemented the following primary factors of operational risk? [Processes]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2= to a smaller degree	3	2.9	2.9	2.9
	3=to a fair degree	7	6.8	6.8	9.7
	4=to a high degree	60	58.3	58.3	68.0
	5=totally	33	32.0	32.0	100.0
	Total	103	100.0	100.0	

Table 8. Processes

Systems:49.5% of the respondents indicated that systems are implemented as primary factor on operational risk in a high degree

To what degree has your organization implemented the following primary factors of operational risk? [Systems]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2= to a smaller degree	4	3.9	3.9	3.9
	3=to a fair degree	6	5.8	5.8	9.7
	4=to a high degree	51	49.5	49.5	59.2
	5=totally	42	40.8	40.8	100.0
	Total	103	100.0	100.0	

Table 9. Systems

External Factors: 45.6 % of the respondents indicated that people is implemented as primary factor on operational risk in a high degree

To what degree has your organization implemented the following primary factors of operational risk? [External factors]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1= not at all	1	1.0	1.0	1.0
	2= to a smaller degree	5	4.9	4.9	5.8
	3=to a fair degree	31	30.1	30.1	35.9
	4=to a high degree	47	45.6	45.6	81.6
	5=totally	19	18.4	18.4	100.0
	Total	103	100.0	100.0	

Table 10. External Factors

4.3.3. Operational Risk Exposures

Each primary risk factor comprises a number of sub factors or exposures that should be managed. The research, therefore, determined to what extent banks recognize various exposures underlying people, processes, systems and external events.

4.3.3.1. People Exposures

The sub factors of the people exposures that were identified in the literature study are the following:

- Incompetence
- Negligence
- Human Error
- Low Morale
- High staff turnover
- Fraudulent activities
- Lack of training

The respondents rated lack of training as the most important sub-factor of people exposure while fraudulent activities were viewed to be second in terms of importance

To what degree has your organization recognized the following people exposures as an important part of operational risk? [Incompetence]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1= not at all	1	1.0	1.0	1.0
	2= to a smaller degree	25	24.3	24.3	25.2
	3=to a fair degree	65	63.1	63.1	88.3
	4=to a high degree	11	10.7	10.7	99.0
	5=totally	1	1.0	1.0	100.0
	Total	103	100.0	100.0	

Table 11. Incompetence

To what degree has your organization recognized the following people exposures as an important part of operational risk? [Negligence]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1= not at all	2	1.9	1.9	1.9
	2= to a smaller degree	3	2.9	2.9	4.9
	3=to a fair degree	25	24.3	24.3	29.1
	4=to a high degree	71	68.9	68.9	98.1
	5=totally	2	1.9	1.9	100.0
	Total	103	100.0	100.0	

Table 12. Negligence

To what degree has your organization recognized the following people exposures as an important part of operational risk? [Human Error]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2= to a smaller degree	8	7.8	7.8	7.8
	3=to a fair degree	47	45.6	45.6	53.4
	4=to a high degree	41	39.8	39.8	93.2
	5=totally	7	6.8	6.8	100.0
	Total	103	100.0	100.0	

Table 13. Human Error

To what degree has your organization recognized the following people exposures as an important part of operational risk? [Low Morale]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1= not at all	4	3.9	3.9	3.9
	2= to a smaller degree	17	16.5	16.5	20.4
	3=to a fair degree	73	70.9	70.9	91.3
	4=to a high degree	7	6.8	6.8	98.1
	5=totally	2	1.9	1.9	100.0
	Total	103	100.0	100.0	

Table 14. Low Morale

To what degree has your organization recognized the following people exposures as an important part of operational risk? [High staff turnover]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1= not at all	4	3.9	3.9	3.9
	2= to a smaller degree	55	53.4	53.4	57.3
	3=to a fair degree	39	37.9	37.9	95.1
	4=to a high degree	3	2.9	2.9	98.1
	5=totally	2	1.9	1.9	100.0
	Total	103	100.0	100.0	

Table 15. High Staff Turnover

To what degree has your organization recognized the following people exposures as an important part of operational risk? [Fraudulent/criminal activities by employees]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2= to a smaller degree	11	10.7	10.7	10.7
	3=to a fair degree	13	12.6	12.6	23.3
	4=to a high degree	43	41.7	41.7	65.0
	5=totally	36	35.0	35.0	100.0
	Total	103	100.0	100.0	

Table 16. Fraudulent/Criminal Activities by Employees

To what degree has your organization recognized the following people exposures as an important part of operational risk? [Lack of training]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1= not at all	2	1.9	1.9	1.9
	2= to a smaller degree	6	5.8	5.8	7.8
	3=to a fair degree	8	7.8	7.8	15.5
	4=to a high degree	25	24.3	24.3	39.8
	5=totally	62	60.2	60.2	100.0
	Total	103	100.0	100.0	

Table 17. Lack of Training

4.3.3.2. Process Exposures

The process exposures that were identifies in the literature study are:

- Errors in process
- Execution errors
- Documentation errors
- Product Complexity
- Security Risks

The respondents rated Security risks as the most important sub-factor of process exposure while errors in procedures and execution errors were viewed to be second in terms of importance.

To what degree has your organization recognized the following process exposures as an important part of operational risk? [Errors in procedures/methodologies]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2= to a smaller degree	3	2.9	2.9	2.9

	3=to a fair degree	8	7.8	7.8	10.7
	4=to a high degree	61	59.2	59.2	69.9
	5=totally	31	30.1	30.1	100.0
	Total	103	100.0	100.0	

Table 18. Errors in procedures/methodologies

To what degree has your organization recognized the following process exposures as an important part of operational risk? [Execution errors]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1= not at all	1	1.0	1.0	1.0
	2= to a smaller degree	1	1.0	1.0	1.9
	3=to a fair degree	9	8.7	8.7	10.7
	4=to a high degree	61	59.2	59.2	69.9
	5=totally	31	30.1	30.1	100.0
	Total	103	100.0	100.0	

Table 19. Execution Errors

To what degree has your organization recognized the following process exposures as an important part of operational risk? [Documentation errors]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2= to a smaller degree	11	10.7	10.7	10.7
	3=to a fair degree	70	68.0	68.0	78.6
	4=to a high degree	21	20.4	20.4	99.0
	5=totally	1	1.0	1.0	100.0
	Total	103	100.0	100.0	

Table 20. Documentation Errors

To what degree has your organization recognized the following process exposures as an important part of operational risk? [Product complexity]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1= not at all	9	8.7	8.7	8.7
	2= to a smaller degree	67	65.0	65.0	73.8
	3=to a fair degree	19	18.4	18.4	92.2
	4=to a high degree	7	6.8	6.8	99.0
	5=totally	1	1.0	1.0	100.0
	Total	103	100.0	100.0	

Table 21. Product Complexity

To what degree has your organization recognized the following process exposures as an important part of operational risk? [Security risks]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2= to a smaller degree	2	1.9	1.9	1.9
	3=to a fair degree	6	5.8	5.8	7.8
	4=to a high degree	44	42.7	42.7	50.5
	5=totally	51	49.5	49.5	100.0
	Total	103	100.0	100.0	

Table 22. Security Risks

4.3.3.3 System Exposures

The process exposures that were identifies in the literature study are:

- System Infiltration
- System Failures
- Fraud
- Programming Errors

- Information Risk
- Telecommunication Risk

The respondents rated Fraud as the most important sub-factor of process exposure while Information Risk was viewed to be second in terms of importance

To what degree has your organization recognized the following system exposures as an important part of operational risk? [System Infiltration]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2= to a smaller degree	15	14.6	14.6	14.6
	3=to a fair degree	75	72.8	72.8	87.4
	4=to a high degree	10	9.7	9.7	97.1
	5=totally	3	2.9	2.9	100.0
	Total	103	100.0	100.0	

Table 23. System Infiltration

To what degree has your organization recognized the following system exposures as an important part of operational risk? [System failures]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2= to a smaller degree	3	2.9	2.9	2.9
	3=to a fair degree	9	8.7	8.7	11.7
	4=to a high degree	84	81.6	81.6	93.2
	5=totally	7	6.8	6.8	100.0
	Total	103	100.0	100.0	

Table 24. System Failures

To what degree has your organization recognized the following system exposures as an important part of operational risk? [Fraud(e.g. Hackers)]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2= to a smaller degree	1	1.0	1.0	1.0
	3=to a fair degree	4	3.9	3.9	4.9
	4=to a high degree	22	21.4	21.4	26.2
	5=totally	76	73.8	73.8	100.0
	Total	103	100.0	100.0	

Table 25. Fraud (e.g. Hackers)

To what degree has your organization recognized the following system exposures as an important part of operational risk? [Programming errors]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2= to a smaller degree	3	2.9	2.9	2.9
	3=to a fair degree	16	15.5	15.5	18.4
	4=to a high degree	51	49.5	49.5	68.0
	5=totally	33	32.0	32.0	100.0
	Total	103	100.0	100.0	

Table 26. Programming Errors

To what degree has your organization recognized the following system exposures as an important part of operational risk? [Information risk]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1= not at all	1	1.0	1.0	1.0

	2= to a smaller degree	2	1.9	1.9	2.9
	3=to a fair degree	7	6.8	6.8	9.7
	4=to a high degree	59	57.3	57.3	67.0
	5=totally	34	33.0	33.0	100.0
	Total	103	100.0	100.0	

Table 27. Information Risk

To what degree has your organization recognized the following system exposures as an important part of operational risk? [Telecommunication risk]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1= not at all	2	1.9	1.9	1.9
	2= to a smaller degree	24	23.3	23.3	25.2
	3=to a fair degree	61	59.2	59.2	84.5
	4=to a high degree	14	13.6	13.6	98.1
	5=totally	2	1.9	1.9	100.0
	Total	103	100.0	100.0	

Table 28. Telecommunication Risk

4.3.3.4. External Exposures

The process exposures that were identifies in the literature study are:

- External criminal activities
- Domestic political disruption
- Regulatory and compliance
- Legal actions
- Business Environment Changes
- Deterioration of bank's reputation as perceived by the market
- Strikes
- Money Laundering

The respondents rated Money Laundering as the most important sub-factor of external exposure while deterioration of bank's reputation as perceived by the market were viewed to be second in terms of importance

To what degree has your organization recognized the following external exposures as an important part of operational risk? [External criminal activities]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1= not at all	1	1.0	1.0	1.0
	2= to a smaller degree	3	2.9	2.9	3.9
	3=to a fair degree	45	43.7	43.7	47.6
	4=to a high degree	48	46.6	46.6	94.2
	5=totally	6	5.8	5.8	100.0
	Total	103	100.0	100.0	

Table 29. External Criminal Activities

To what degree has your organization recognized the following external exposures as an important part of operational risk? [Domestic political disruption]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1= not at all	3	2.9	2.9	2.9
	2= to a smaller degree	34	33.0	33.0	35.9
	3=to a fair degree	57	55.3	55.3	91.3
	4=to a high degree	6	5.8	5.8	97.1
	5=totally	3	2.9	2.9	100.0
	Total	103	100.0	100.0	

Table 30. Domestic Political Disruption

To what degree has your organization recognized the following external exposures as an important part of operational risk? [Regulatory and compliance]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2= to a smaller degree	1	1.0	1.0	1.0
	3=to a fair degree	8	7.8	7.8	8.7
	4=to a high degree	58	56.3	56.3	65.0
	5=totally	36	35.0	35.0	100.0
	Total	103	100.0	100.0	

Table 31. Regulatory and Compliance

To what degree has your organization recognized the following external exposures as an important part of operational risk? [Legal actions]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2= to a smaller degree	1	1.0	1.0	1.0
	3=to a fair degree	6	5.8	5.8	6.8
	4=to a high degree	67	65.0	65.0	71.8
	5=totally	29	28.2	28.2	100.0
	Total	103	100.0	100.0	

Table 32. Legal Actions

To what degree has your organization recognized the following external exposures as an important part of operational risk? [Business environment changes]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1= not at all	1	1.0	1.0	1.0
	2= to a smaller degree	39	37.9	37.9	38.8
	3=to a fair degree	47	45.6	45.6	84.5
	4=to a high degree	13	12.6	12.6	97.1
	5=totally	3	2.9	2.9	100.0
	Total	103	100.0	100.0	

Table 33. Business Environment Changes

To what degree has your organization recognized the following external exposures as an important part of operational risk? [Deterioration of a bank's reputation as perceived by the market]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2= to a smaller degree	2	1.9	1.9	1.9
	3=to a fair degree	8	7.8	7.8	9.7
	4=to a high degree	50	48.5	48.5	58.3
	5=totally	43	41.7	41.7	100.0
	Total	103	100.0	100.0	

Table 34. Deterioration of a bank's reputation as perceived by the market

To what degree has your organization recognized the following external exposures as an important part of operational risk? [Strikes]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1= not at all	74	71.8	71.8	71.8
	2= to a smaller degree	11	10.7	10.7	82.5
	3=to a fair degree	6	5.8	5.8	88.3
	4=to a high degree	7	6.8	6.8	95.1
	5=totally	5	4.9	4.9	100.0
	Total	103	100.0	100.0	

Table 35. Strikes

To what degree has your organization recognized the following external exposures as an important part of operational risk? [Money laundering]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2= to a smaller degree	1	1.0	1.0	1.0
	3=to a fair degree	5	4.9	4.9	5.8
	4=to a high degree	26	25.2	25.2	31.1
	5=totally	71	68.9	68.9	100.0
	Total	103	100.0	100.0	

Table 36. Money Laundering

4.3.4. Operational Risk Management Process

According to the literature review the management of operational risks can be described as a cycle included of the following steps:

- Risk identification,
- Risk assessment,
- Risk control,
- Risk monitoring

4.3.4.1. Operational Risk Management Elements

A bank should first be aware of the potential risks to be able to control and limit its risks. A bank can take a preventive measure by identifying and assessing the risks. The methods a bank can use for prevention is the Risk Identification and Risk assessment.

The responders in the question "To what degree has your organization recognized the following as important elements of an operational risk management process?" rated the Risk Assessment as the most important element of an operational risk management process whereas risk identification was viewed to be second in terms of importance.

According to the literature, a very important component of risk management is Risk assessment because it provides the foundation for many parts in the risk management cycle. Specifically, risk assessment can be help the organization to establish suitable policies, to pick cost effective techniques to implement them. Organizations should assess risks due to the reason can be changed gradually and adjust the strategy on policies and control to best handle the related risk (U.S. GAO 1999; Stoneburner et al 2002).

To what degree has your organization recognized the following as important elements of an operational risk management process? [Risk Identification]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2= to a smaller degree	2	1.9	1.9	1.9
	3=to a fair degree	6	5.8	5.8	7.8
	4=to a high degree	63	61.2	61.2	68.9
	5=totally	32	31.1	31.1	100.0
	Total	103	100.0	100.0	

Table 37. Risk Identification

To what degree has your organization recognized the following as important elements of an operational risk management process? [Risk Assessment]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2= to a smaller degree	3	2.9	2.9	2.9
	3=to a fair degree	6	5.8	5.8	8.7
	4=to a high degree	26	25.2	25.2	34.0
	5=totally	68	66.0	66.0	100.0
	Total	103	100.0	100.0	

Table 38. Risk Assessment

To what degree has your organization recognized the following as important elements of an operational risk management process? [Risk Control]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2= to a smaller degree	2	1.9	1.9	1.9
	3=to a fair degree	13	12.6	12.6	14.6
	4=to a high degree	83	80.6	80.6	95.1
	5=totally	5	4.9	4.9	100.0
	Total	103	100.0	100.0	

Table 39. Risk Control

To what degree has your organization recognized the following as important elements of an operational risk management process? [Risk Monitoring]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2= to a smaller degree	5	4.9	4.9	4.9
	3=to a fair degree	76	73.8	73.8	78.6
	4=to a high degree	16	15.5	15.5	94.2
	5=totally	6	5.8	5.8	100.0
	Total	103	100.0	100.0	

Table 40. Risk Monitoring

4.3.4.2. Importance of Operational Risk Management Process

In the questions that concern to what degree does your organization recognized the importance of aligning an operational risk management process with its strategy and objectives most of responders believe that is Significant Important (67%).

All banking products, activities, processes and systems are included in Operational Risk. A crucial element of bank's risk management is the effective management of operational risk. Thus, an operational risk management reflects the effectiveness on board and senior management in administering its portfolio of products, activities, processes, and systems (Basel Committee on Banking Supervision, 2011).

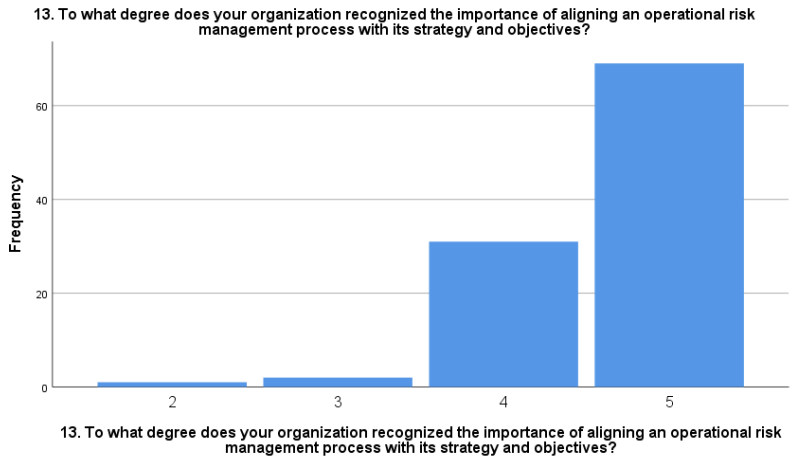

Figure 7. Importance of Operational Risk

4.3.4.3. Risk Assessment, an ongoing process

In the questions that concern to what degree has your organization recognized the implementation of risk assessment as an important ongoing process, most of the responders believe that is Significant Important (67%).

Risk assessment is overall process of hazard identification, risk analysis, and risk evaluation. The first step is to identify the risks arising, then the risks are analyzed in term of their probability and consequences. At the end, based on the outcomes of risk assessment process, the decision makers can decided if an activity should be undertaken, appropriate selection of risk treatment strategies, whether risks need to be reduced or eliminated (ISO 17776, 2000; IEC, 2008, AS/NZS: 4360, 2004).

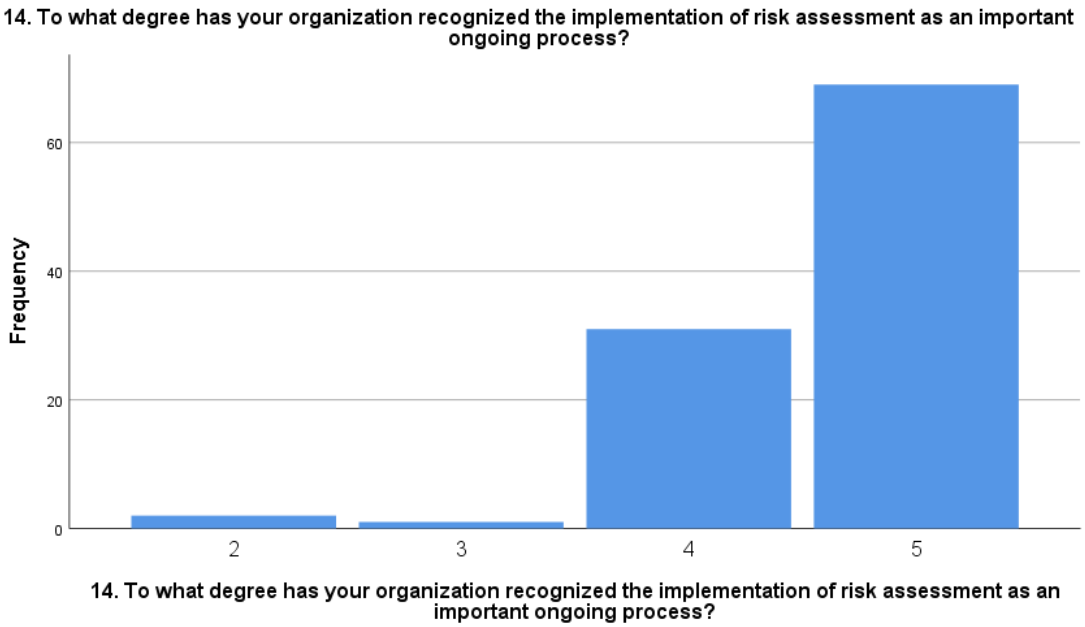

Figure 8. Risk Assessment Implementation

4.4. Cyber Threats and External Fraud in the Banking Industry

In the last section of the questionnaire explores the two of the most significant Operational Risks of banking sector, Cyber Threats and External Fraud, over the last decade.

4.4.1. The problem of external fraud and cyber risk

The respondents in the question how employees classify the problem of external fraud and cyber risk in the banking industry, as figure illustrates, the 98.1% said that is a “Major Problem”.

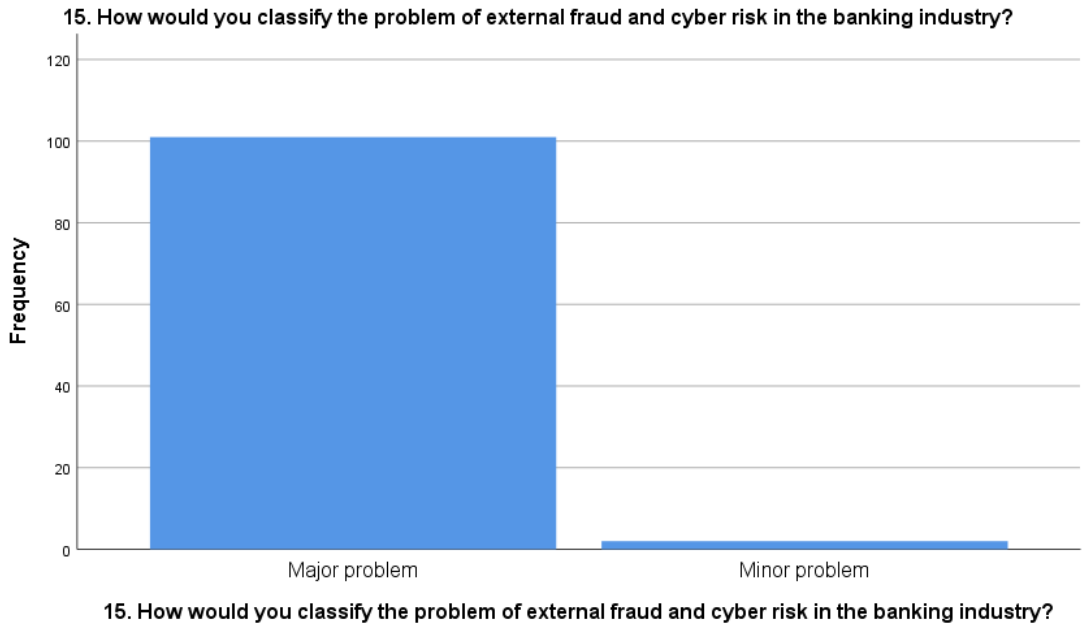

Figure 9. External Fraud and Cyber Risk

4.4.2. Likelihood of external fraud and cyber threats over the next five years

The respondents in the question about the likelihood of external fraud and cyber threats over the next five years, as figure illustrates, the 93.2% said that is “Very likely”.

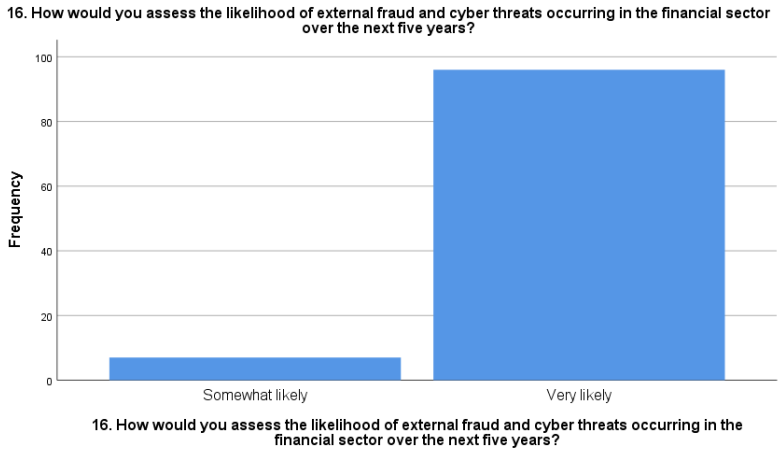

Figure 10. Likelihood

4.4.3. Direction of trend in external fraud and cyber risk

The third question focused on the direction of the trend in fraud. Seventeen-four respondents (71.8%) indicated that it was increasing rapidly, while twenty – three (25.2%) indicated that it was increasing. Three respondents (2.9%) indicated that was remaining constant.

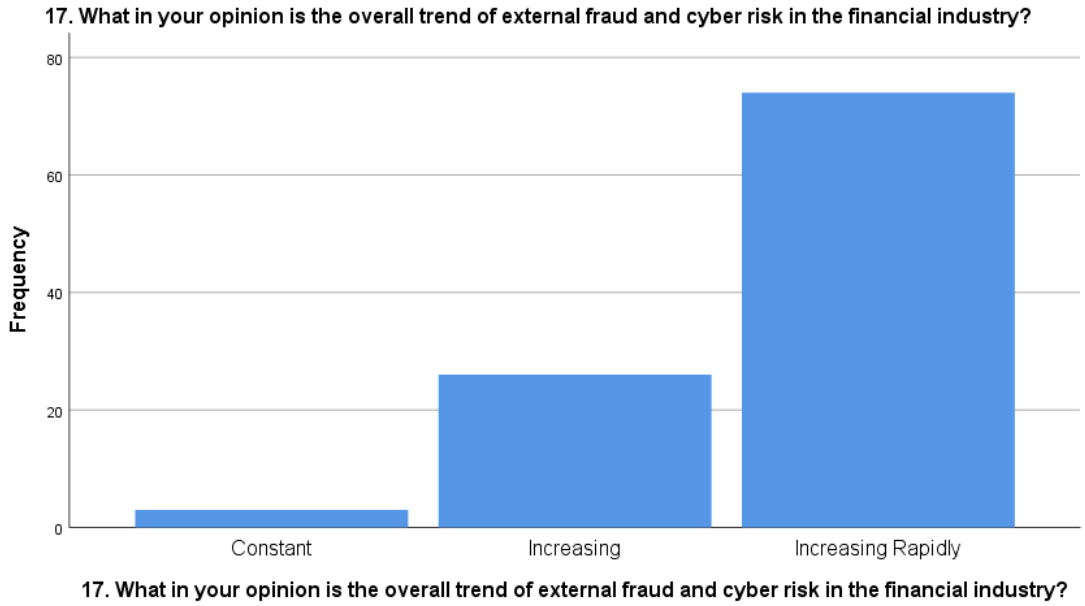

Figure 11. Direction

Cyber threats continue to be critical issues among industries. Cyber threats are unavoidable and unpredictable, because of increasing deleterious financial and reputation impacts. Cyber-attacks are estimated occurs 1.5. Million in an annual basis (CBS, 2015), which means that cyber-crime is a constant threat to any person, business, government, and organization.

A survey from Price Water House Coopers (2014) found that cybercrime was the second most common type of economic crime. In the same survey, the 39%of cybercrime reporting was from financial sector (PWC, 2014).

Research shows that all financial organization faced a fraud threat, and that the typical organization loses 5-7% of its annual revenues to fraud. (Samociuk, Iyer & Doody, 2010)

4.4.4. Factors Connected with External Fraud

This question focused on the respondent identifying the organizational factors connected to External Fraud. Table indicates the factors connected with the External Fraud.

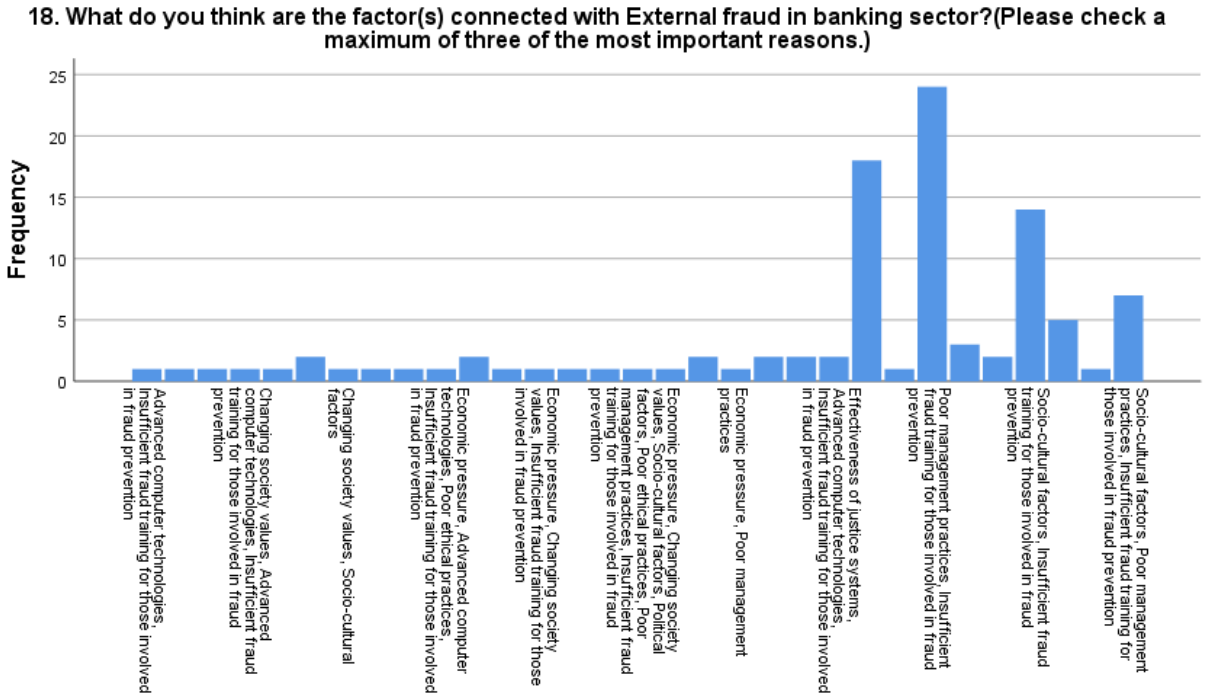

Figure 12. External Fraud Factors

The result shows that 87.4% of the respondents believes that Insufficient Fraud training for those involved in fraud is a very important factor connected in External Fraud. According to Shongola (1994), Insufficient Staff Training could affect the Fraud event. Lack of knowledge of the ways of dealing with fraudulent practices in banks could affect avoiding fraudulent events.

4.4.5. Bank's Poor Management

Seventeen-two of respondents (69.8 %) strongly agree with the statement that Banks with poor management record higher incidence of all sorts of fraud that those with effective management.

Shongola (1994) argued that banks with poor management record a higher incidence of frauds than those with effective management. Poor management has as a result a poor control system, indiscipline among staff and this create an environment for increasing fraud's events.

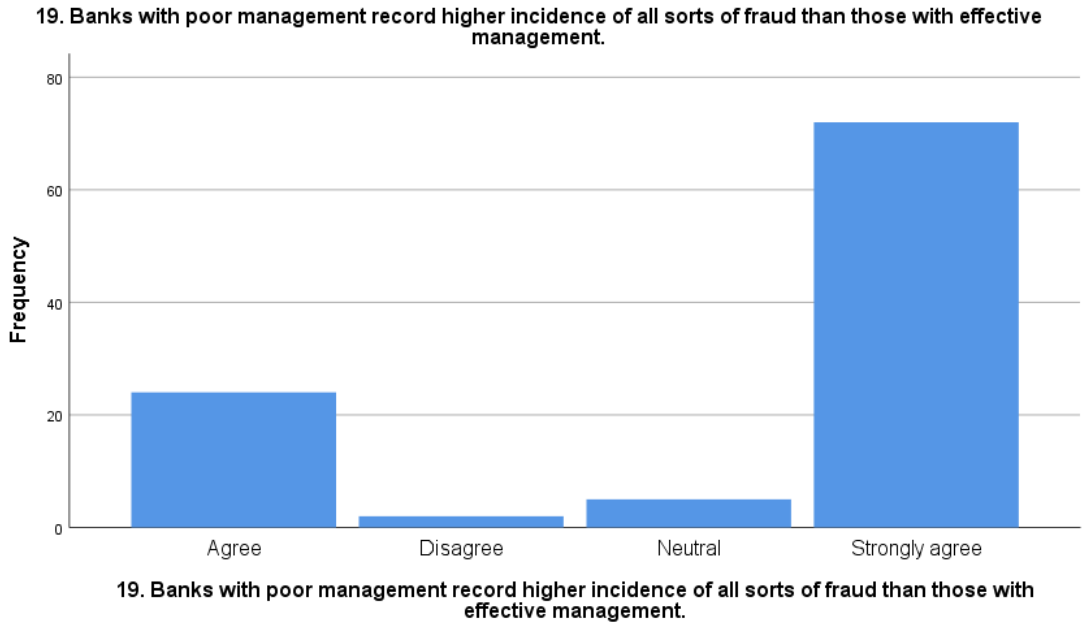

Figure 13. Poor Management

4.4.6. Causes of fraud

The 96.1% of the responders believed that the causes of bank fraud are:

- Poor Security Management, Staff Negligence and Poor Security Arrangement.
- According to Nweze (2008), Banks with poor security arrangement for valuable documents, it is easy for fraudsters to have access undirected in the bank.

- Songola (1994), said that staff negligence could contribute to fraud in banks. Negligence composed from several factors including poor supervision, lack of technical knowledge, apathy and pressure, lack of experience.

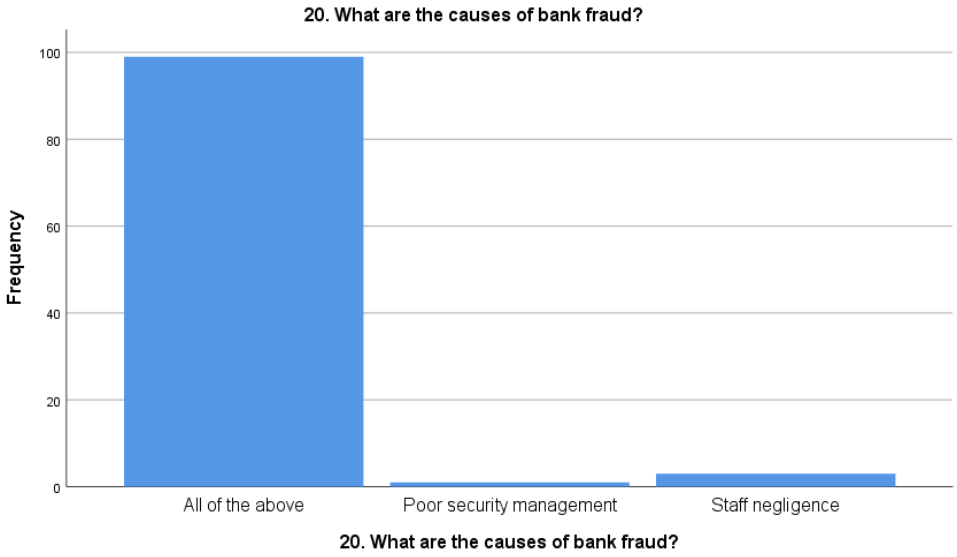

Figure 14. Causes of fraud

4.4.7. Factors detecting and controlled fraud

Figure indicates that 96.1% of the respondents believe that the factors affecting and controlled fraud are: personnel and administrative control, accounting and financial control and inventory and process control.

Shogotola (1994) identifies the below factors for detecting and controlled fraud

- Personnel Control: Proper recruitment procedure, Proper Disengagements Procedure, Positing and Placement.
- Administrative Control: Segregation of duties, Dual custody, Movement logs and registers, Access rights and restrictions, Security personnel, Passwords.
- Accounting Control: Data validation, prompt positing of transaction, Balancing, Reconciliation, Variance analyst, Reviews and statistics.

Figure 15. Fraud detection &controlled

4.4.8. The Significance of External Fraud and Cyber Risk as Operational Risk Factor

In the question that concern how significant is External fraud as operational risk factor for your bank most responders believe that is Very Significant (82.5%). As for Cyber Threats 80.06% of responders think that is Very Significant operational risk factor

The Basel Committee for Bank Supervision (2011), categorize External Fraud as one of the seven categories of Operational Risk. Further, according to the Risk. Net, External Fraud and Cyber Threats are two of the10 Operational Risks for 2017(2017, Jan 23).

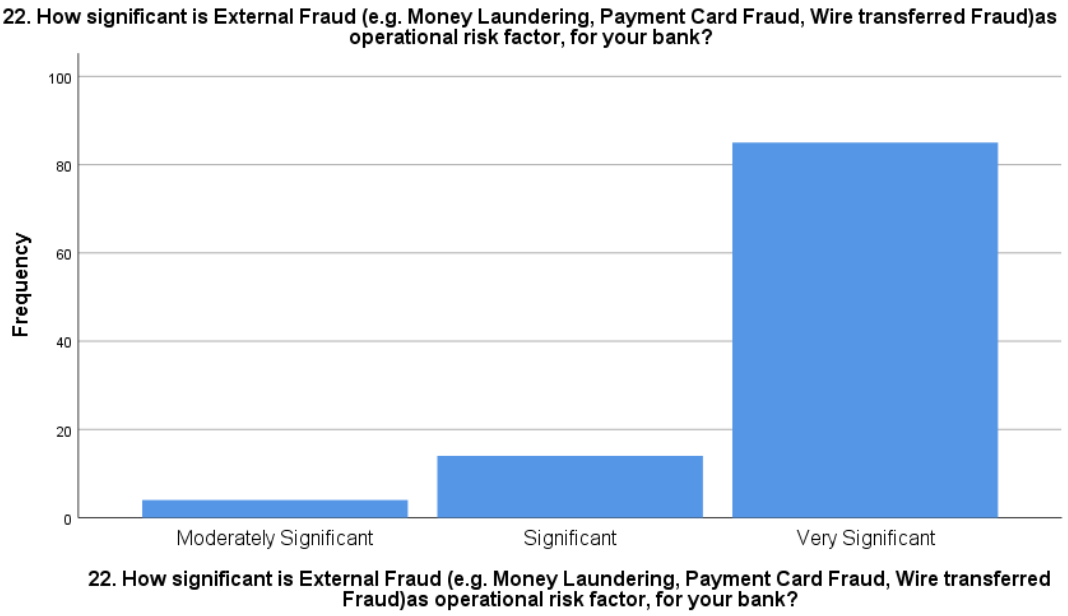

Figure 16. External Fraud Significant

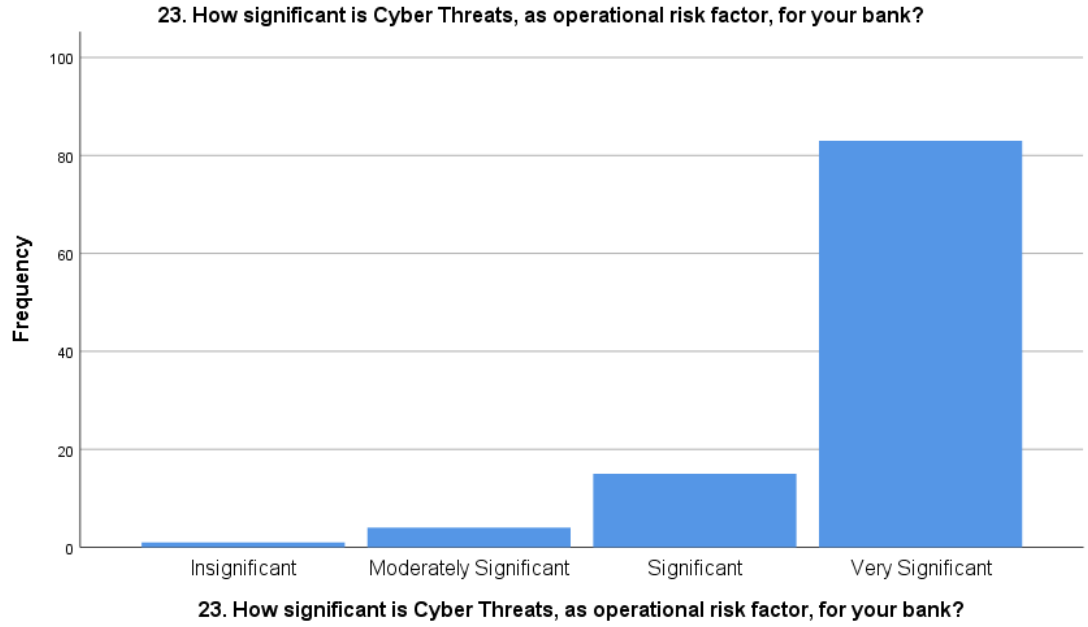

Figure 17. Cyber Threats Significant

4.4.9. Factors Connected with Cyber Threats

This question focused on the respondent identifying the organizational factors connected to External Fraud. Table indicates the factors connected with the External Fraud.

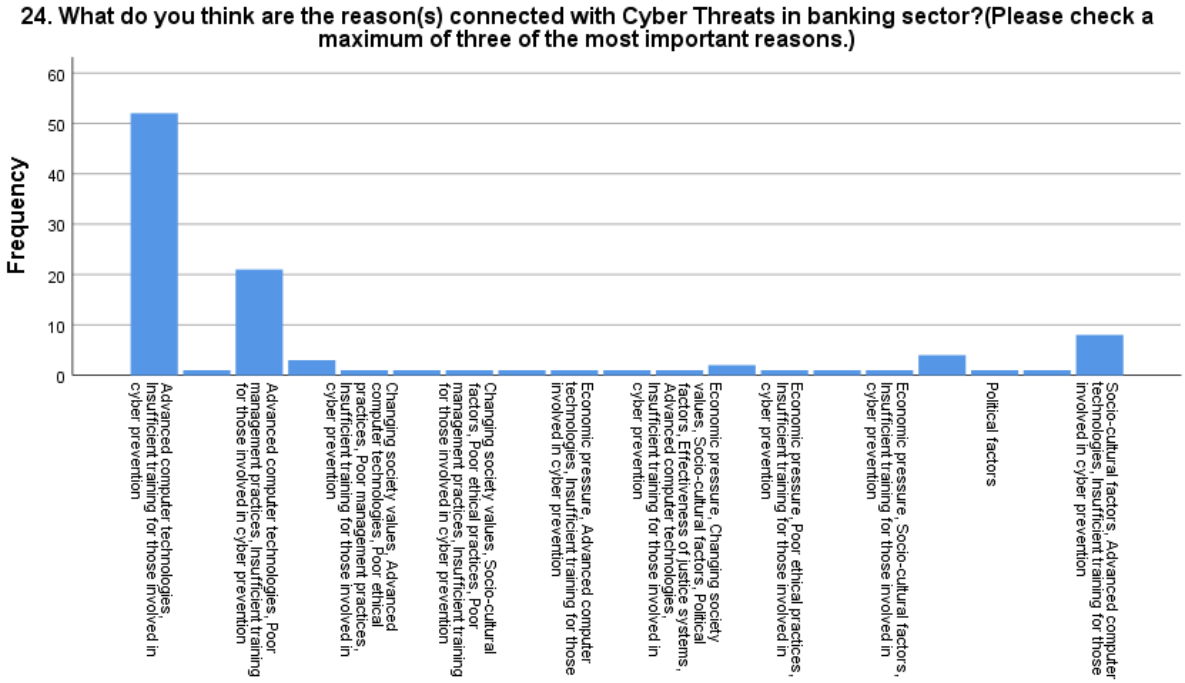

Figure 18. Cyber Threats Factors

The result shows that 92.2 % of the respondents believes that insufficient training for those involved in cyber prevention and Advanced Computer technologies is a very important factor connected in Cyber Threats.

According to a research which ISC completed (September 2017), most organization do not provide sufficient resources for training and development.

4.4.10. Motives of the attacker

Figure indicates that 48.5 % of the respondents believe that the motives of attackers of cyber threat is unwelcome malicious damage.29.1% of the respondents think that attackers motive is the illegal financial gain.

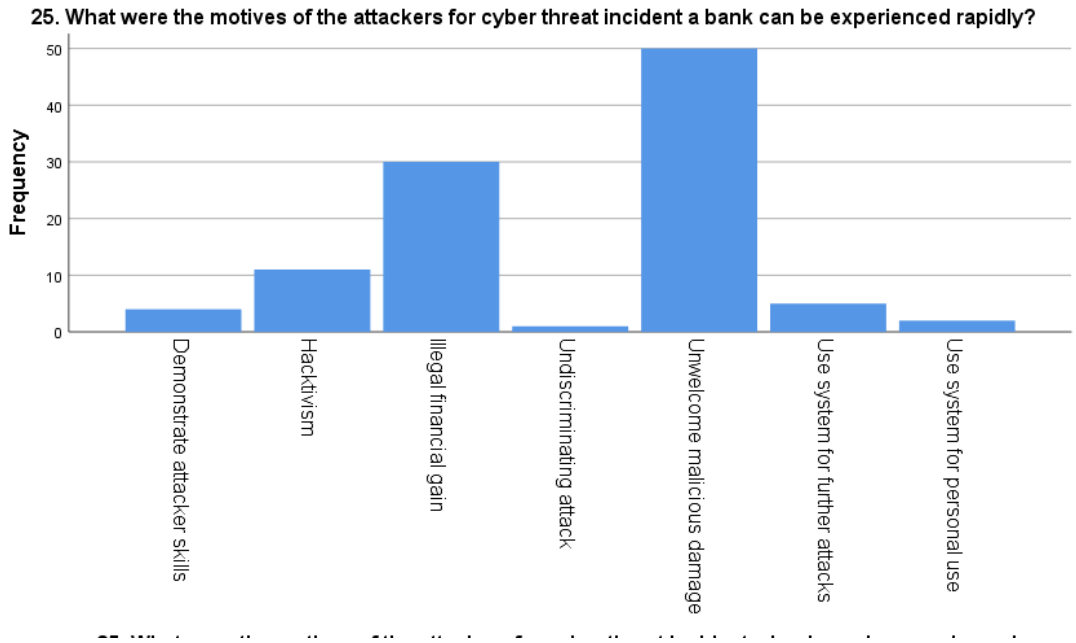

Figure 19. Motives of the attackers

4.4.11. Factors Causes Cyber Risk

Figure indicates that 88.3% of the respondents believe that the lack of security technologies contributes to Cyber risk. A high percentage of factor causes Cyber Risk has the insufficient staff training variable, with 86.4%.

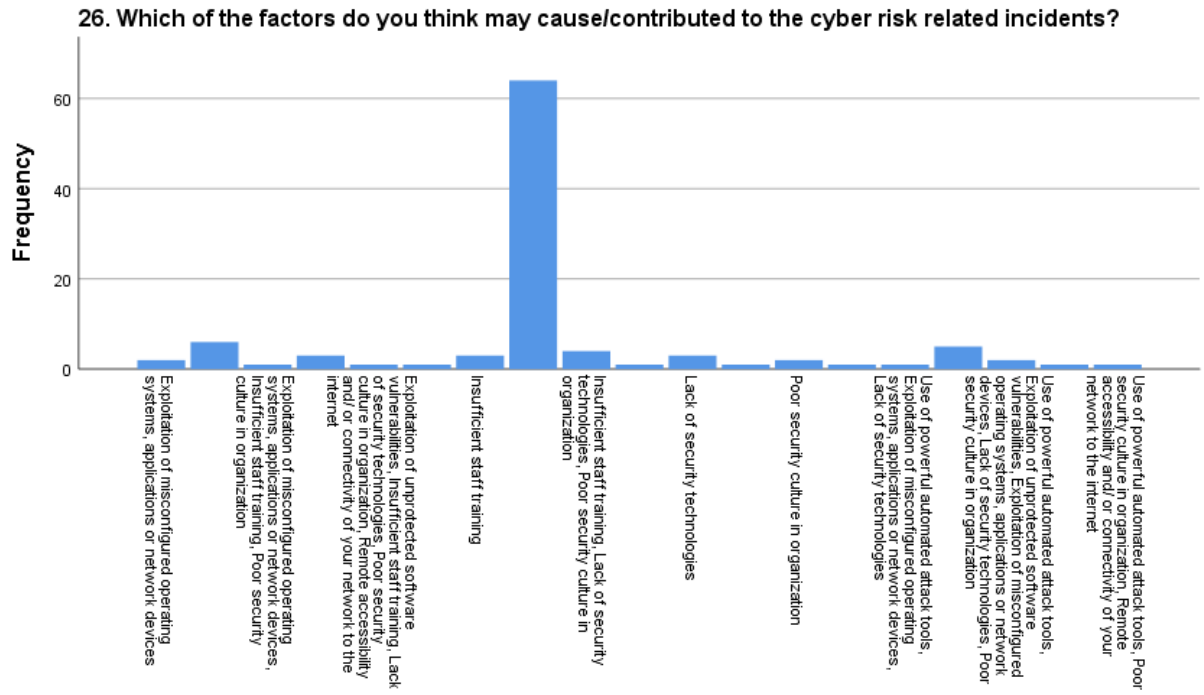

Figure 20. Causes of Cyber Threats

4.4.12. Business Continuity Plan

The next four questions are about the Business Continuity plan.

The 83.5% of respondents have Business Continuity plan within their organization for encounter cyber threats. Further, 99% of bank employees believes that their organization has preparedness a business continuity plan for external fraud and cyber risk incidents. In addition to this, the 89.3% of respondents claims that their organization's business continuity plan is adequate and effective enough to ensure that critical operations of the bank are resumed as quickly as possible in an event of a cyber threat and external fraud.

In the question "In your opinion, in case of cyber threat and external fraud occur within your bank, if the process of the Business continuity plan, is not performed within the recovery time objective, what would be the impact for the bank?" 59.2% of the responders answered that the impact of the bank will be "Reputation" and the 33% "Compliance and Legal"

The Business Continuity Institute (BCI, 2007) defines BCM as:

'A holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience with the capability for an effective response that safeguards the interests of key stakeholders, reputation, brand & value creating activities.' Business continuity planning is recognized from Shaw and Harrald (2004) as a very important aspect off business continuity management. Business continuity planning involves of business practices that provide guidance for the decisions and actions required for a firm to prevent, mitigate, prepare for, respond to, resume, recover, restore, and transition from a crisis event. Generally, organizations which had a plan in place during a disaster event, could resume operations very quickly whereas those who did not have any plan.

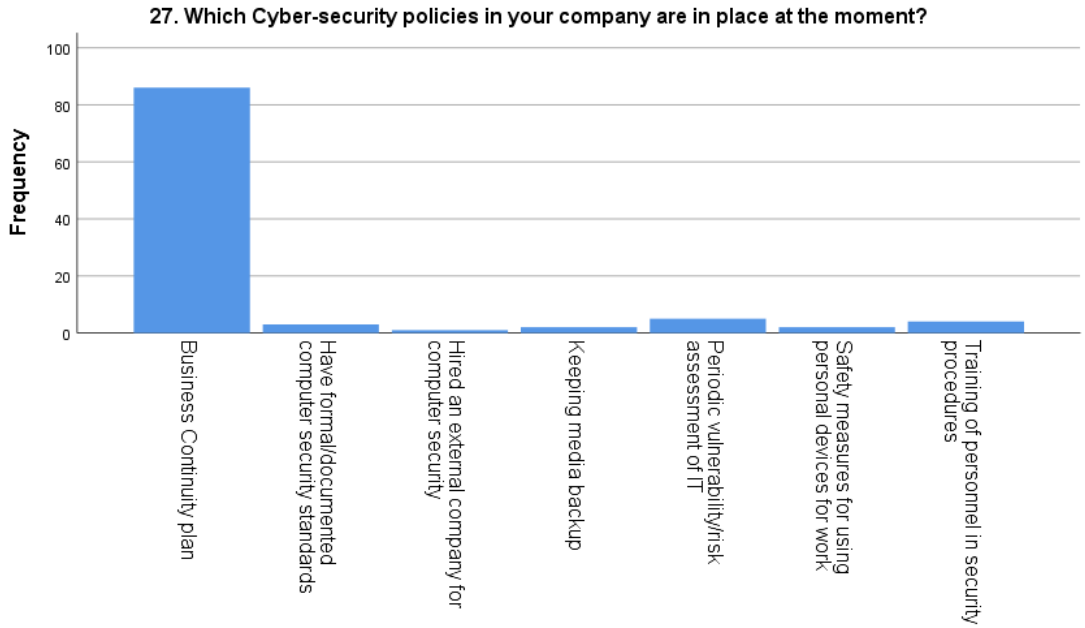

Figure 21. Cyber security policies

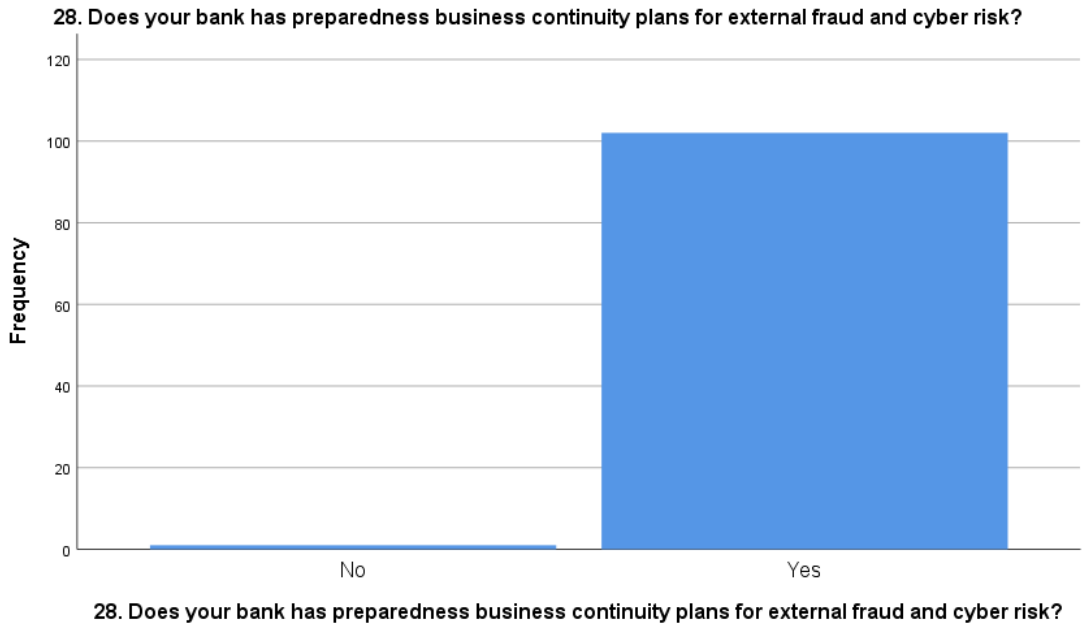

Figure 22. Business Continuity plan

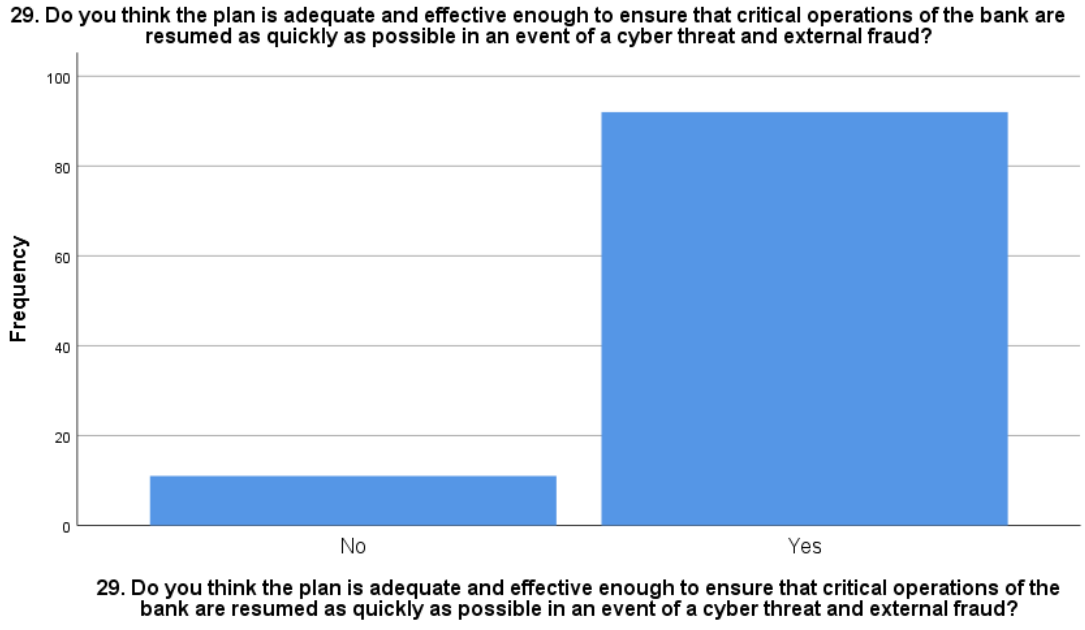

Figure 23. Effective Business Continuity

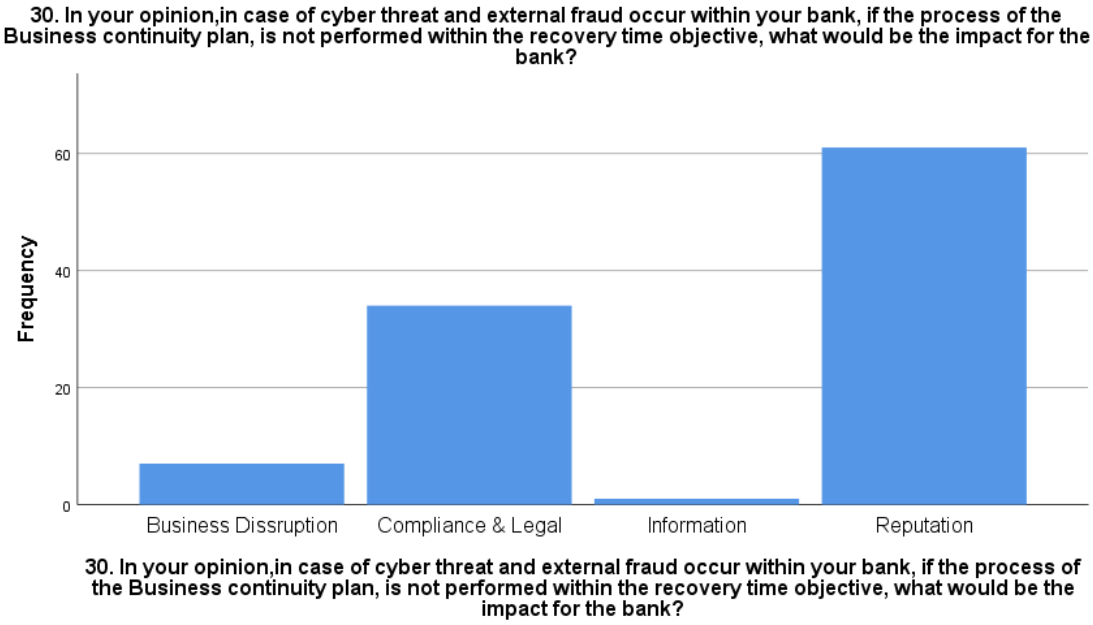

Figure 24. Impact of BCP

4.5. Factors Connected with Cyber Risk and Fraud

4.5.1. Factors Connected with Cyber Risk

Correlation analyses were conducted to examine the relationship between the factors connected with Cyber Risk.

Correlations

		cyber risk	People	processes	systems	external factors
cyber risk	Pearson Correlation	1	.472**	.447**	.519**	.521**
	Sig. (2-tailed)		.000	.000	.000	.000
	N	103	103	103	103	103

**. Correlation is significant at the 0.01 level (2-tailed).

Table 41. Correlation Analysis between factors connected with Cyber Risk

The table summarizes the descriptive statistics and analysis results. As it can be seen all the factors have moderate positive linear relationship.

Correlations between Cyber Risk and People exposures

		cyber risk
Incompetence	Pearson Correlation	-.098
	Sig. (2-tailed)	.323
	N	103
Negligence	Pearson Correlation	.452**
	Sig. (2-tailed)	.000
	N	103
human error	Pearson Correlation	.198*
	Sig. (2-tailed)	.045
	N	103
low morale	Pearson Correlation	.005
	Sig. (2-tailed)	.960
	N	103
high staff turnover	Pearson Correlation	-.056
	Sig. (2-tailed)	.575
	N	103
fraudulent/criminal activities by employees	Pearson Correlation	.258**
	Sig. (2-tailed)	.008
	N	103
lack of training	Pearson Correlation	.672**
	Sig. (2-tailed)	.000

	N	103

Table 42. Correlations between Cyber Risk and People exposures

Correlation analyses were conducted to examine the relationship between People Exposures (Incompetence, Negligence, Human Error, Low Morale, High staff turnover, Fraudulent/criminal activities by employees, Lack of training) with Cyber Risk. As shown in the table Incompetence has strong negative relationship with Cyber Risk, Negligence indicate a moderate positive linear relationship with Cyber Risk, Human Error, Low Morales and Fraudulent/criminal activities by employees have a weak positive linear relationship with Cyber Risk. Moreover, High staff turnover has a negative moderate relationship with Cyber Risk and Lack of training has a moderate positive linear relationship with Cyber Risk.

Correlations between Process Exposures and Cyber Risk

		cyber risk
errors in procedures/methodologies	Pearson Correlation	.569**
	Sig. (2-tailed)	.000
	N	103
execution errors	Pearson Correlation	.406**
	Sig. (2-tailed)	.000
	N	103
documentation errors	Pearson Correlation	-.100
	Sig. (2-tailed)	.317
	N	103
product complexity	Pearson Correlation	-.424**
	Sig. (2-tailed)	.000
	N	103

security risks	Pearson Correlation	.552**
	Sig. (2-tailed)	.000
	N	103

Table 43. Correlations between Process Exposures and Cyber Risk

Correlation analyses were conducted to examine the relationship between Process Exposures (Errors in procedures/methodologies, execution errors, documentation errors, product complexity, Security risks) with Cyber Risk. As shown in the table Errors in procedures/methodologies, execution errors and security risks have a moderate positive linear relationship with Cyber Risk, Documentation errors indicate a weak negative linear relationship with Cyber Risk and last Product Complexity has a moderate negative linear relationship with Cyber Risk.

Correlations between System Exposures and Cyber Risk

		cyber risk
system infiltration	Pearson Correlation	-.231*
	Sig. (2-tailed)	.019
	N	103
system failures	Pearson Correlation	.348**
	Sig. (2-tailed)	.000
	N	103
fraud(e.g. hackers)	Pearson Correlation	.617**
	Sig. (2-tailed)	.000
	N	103
programming errors	Pearson Correlation	.470**
	Sig. (2-tailed)	.000

	N	103
information risk	Pearson Correlation	.512**
	Sig. (2-tailed)	.000
	N	103
telecommunication risk	Pearson Correlation	-.176
	Sig. (2-tailed)	.076
	N	103

Table 44. Correlations between System Exposures and Cyber Risk

Correlation analyses were conducted to examine the relationship between System Exposures (System Infiltration, System failures, Fraud (e.g. Hackers), Programming errors, Information risk, and Telecommunication risk) with Cyber Risk. As shown in the table there is a weak negative linear relationship between Telecommunication Risk- System Infiltration with Cyber Risk. Fraud, Programming errors and Information Risk have a moderate positive linear relationship with Cyber Risk. Further, System failures indicate a weak positive relationship with Cyber Risk

Correlations between External Exposures and Cyber Risk

		cyber risk
external criminal activities	Pearson Correlation	.142
	Sig. (2-tailed)	.153
	N	103
domestic political disruption	Pearson Correlation	-.223*
	Sig. (2-tailed)	.023
	N	103

regulatory and compliance	Pearson Correlation	.196*
	Sig. (2-tailed)	.047
	N	103
legal actions	Pearson Correlation	.242*
	Sig. (2-tailed)	.014
	N	103
business environment changes	Pearson Correlation	-.425**
	Sig. (2-tailed)	.000
	N	103
deterioration of a bank's reputation as perceived by the market	Pearson Correlation	.365**
	Sig. (2-tailed)	.000
	N	103
Strikes	Pearson Correlation	-.427**
	Sig. (2-tailed)	.000
	N	103
money laundering	Pearson Correlation	.580**
	Sig. (2-tailed)	.000
	N	103

Table 45. Correlations between External Exposures and Cyber Risk

Correlation analyses were conducted to examine the relationship between External Exposures (external criminal activities, domestic political disruption, regulatory and compliance, legal actions, business environment changes, deterioration of a bank's reputation as perceived by the market, Strikes, money laundering) with Cyber Risk. As shown in the table there is a weak negative linear relationship between Domestic political disruptions with Cyber Risk.

Strikes and Business environment changes has moderate negative linear relationship with Cyber Risk. External criminal activities, Regulatory and compliance and legal actions have a weak positive linear relationship with Cyber Risk. Moreover, Cyber Risk and Deterioration of bank's reputation as perceived by the market and Money laundering have a moderate positive linear relationship with Cyber Risk.

4.5.2. Factors Connected with Fraud In the banking sector

Correlations between Factors Connected with Fraud In the banking sector

		Fraud	People	Processes	systems	external factors
Fraud	Pearson Correlation	1	.273**	.329**	.485**	.485**
	Sig. (2-tailed)		.005	.001	.000	.000
	N	103	103	103	103	103

Table 46. Correlations between Factors Connected with Fraud In the banking sector

Correlation analyses were conducted to examine the relationship between the factors People, Processes, Systems, External Factors connected with Fraud in the banking sector. As shown in the table People and Processes have a weak positive linear relationship with Fraud. Additionally, Systems and External factors have a moderate positive linear relationship with the score of Fraud.

Correlations Between People Exposures and Fraud

		Fraud
Incompetence	Pearson Correlation	-.093
	Sig. (2-tailed)	.348
	N	103
Negligence	Pearson Correlation	.339**
	Sig. (2-tailed)	.000

	N	103
human error	Pearson Correlation	.164
	Sig. (2-tailed)	.098
	N	103
low morale	Pearson Correlation	-.003
	Sig. (2-tailed)	.973
	N	103
high staff turnover	Pearson Correlation	-.094
	Sig. (2-tailed)	.346
	N	103
fraudulent/criminal activities by employees	Pearson Correlation	.160
	Sig. (2-tailed)	.106
	N	103
lack of training	Pearson Correlation	.482**
	Sig. (2-tailed)	.000
	N	103

Table 47. Correlations between People Exposures and Fraud

Correlation analyses were conducted to examine the relationship between the People exposures and Fraud in the banking sector. As shown in the table Incompetence, Low morale, High staff turnover have no relation with Fraud. Additionally, Negligence, Lack of training have a moderate positive linear relationship with the score of Fraud and Human error, Fraudulent/criminal activities by employees have weak positive linear relationship with Fraud.

Correlations between Process Exposures and Fraud

		fraud
errors in procedures/methodologies	Pearson Correlation	.397**
	Sig. (2-tailed)	.000
	N	103
execution errors	Pearson Correlation	.224*
	Sig. (2-tailed)	.023
	N	103
documentation errors	Pearson Correlation	-.174
	Sig. (2-tailed)	.079
	N	103
product complexity	Pearson Correlation	-.427**
	Sig. (2-tailed)	.000
	N	103
security risks	Pearson Correlation	.499**
	Sig. (2-tailed)	.000
	N	103

Table 48. Correlations between Process Exposures and Fraud

Correlation analyses were conducted to examine the relationship between Process Exposures (Errors in procedures/methodologies, execution errors, documentation errors, product complexity, Security risks) with Fraud. As shown in the table Errors in procedures/methodologies and Security Risks have a moderate positive linear relationship with Fraud and Execution errors indicate a weak positive linear relationship with Fraud. Documentation errors has a weak negative linear relationship with Fraud and last Product Complexity has a moderate negative linear relationship with Fraud.

Correlations System Exposures and Fraud

	Fraud

system infiltration	Pearson Correlation	-.058
	Sig. (2-tailed)	.561
	N	103
system failures	Pearson Correlation	.400**
	Sig. (2-tailed)	.000
	N	103
fraud(e.g. hackers)	Pearson Correlation	.598**
	Sig. (2-tailed)	.000
	N	103
programming errors	Pearson Correlation	.404**
	Sig. (2-tailed)	.000
	N	103
information risk	Pearson Correlation	.489**
	Sig. (2-tailed)	.000
	N	103
telecommunication risk	Pearson Correlation	-.077
	Sig. (2-tailed)	.442
	N	103

Table 49. Correlations System Exposures and Fraud

Correlation analyses were conducted to examine the relationship between System Exposures (System Infiltration, System failures, Fraud (e.g. Hackers), Programming errors, Information risk, and Telecommunication risk) with Fraud Risk. As shown in the table there is a weak negative linear relationship between Telecommunication Risk and Fraud but System Infiltration has strong negative linear relationship with Fraud. System failures, Information risk have moderate

positive linear relationship with Fraud and Fraud (e.g. hackers) has strong positive linear relationship with Fraud.

Correlations between External Exposures and Fraud

		Fraud
external criminal activities	Pearson Correlation	.187
	Sig. (2-tailed)	.058
	N	103
domestic political disruption	Pearson Correlation	-.103
	Sig. (2-tailed)	.300
	N	103
regulatory and compliance	Pearson Correlation	.139
	Sig. (2-tailed)	.161
	N	103
legal actions	Pearson Correlation	.129
	Sig. (2-tailed)	.192
	N	103
business environment changes	Pearson Correlation	-.290**
	Sig. (2-tailed)	.003
	N	103
deterioration of a bank's reputation as perceived by the market	Pearson Correlation	.311**
	Sig. (2-tailed)	.001
	N	103
Strikes	Pearson Correlation	-.178

	Sig. (2-tailed)	.071
	N	103
money laundering	Pearson Correlation	.558**
	Sig. (2-tailed)	.000
	N	103

Table 50. Correlations between External Exposures and Fraud

Correlation analyses were conducted to examine the relationship between External Exposures

(External criminal activities, domestic political disruption, regulatory and compliance, legal actions, business environment changes, deterioration of a bank's reputation as perceived by the market, Strikes, money laundering) with Fraud. As shown in the table there is a weak negative linear relationship between Domestic political disruption, business environment, changes, and strikes with Fraud. External criminal activities, regulatory and compliance, legal actions have a weak positive linear relationship with Fraud. Moreover, Fraud Risk and Deterioration of bank's reputation as perceived by the market has moderate positive linear relationship. Last, Money Laundering has strong positive relationship with Fraud.

4.6. Risk Assessment and operational risk management process

		13. To what degree does your organization recognized the importance of aligning an operational risk management process with its strategy and objectives?
14. To what degree has your organization recognized the implementation of risk assessment as an important ongoing process?	Pearson Correlation	.933**
	Sig. (2-tailed)	.000
	N	103

Table 51. Correlation of Risk Assessment and Operational Risk

Correlational analyses were used to examine the relationship between the risk assessment and operational risk management process. Results indicated a strong positive linear relationship via risk assessment and operational risk management process.

4.7. Relationship between Fraud and Cyber Risk, as factors, with effective Business Continuity Planning

Fraud * effective business continuity planning

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	24.632[a]	3	.000
Likelihood Ratio	15.062	3	.002
Linear-by-Linear Association	6.901	1	.009
N of Valid Cases	103		

a. 4 cells (50.0%) have expected count less than 5. The minimum expected count is .11.

Table 52. Chi – Square Test of Fraud and Business Continuity Planning

A chi-square test was performed and there is a significant relationship between Fraud and Effective continuity planning.

Cyber risk* effective business continuity planning

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	16.021[a]	3	.001
Likelihood Ratio	11.029	3	.012
Linear-by-Linear Association	11.721	1	.001

N of Valid Cases	103		
a. 4 cells (50.0%) have expected count less than 5. The minimum expected count is .21.			

Table 53. Chi – Square Test of Cyber Threats and Business Continuity Planning

A chi-square test was performed and there is a significant relationship between Cyber Risks and Effective continuity planning.

4.8. Qualitative Results

The questions conducted from: two supervisors (S1 & S2), one manager (M1), one Sub Department manager (SM1) and a Customer Support officer (SO1)

The questions were about:

- How long have you been employed on your organization?
- What is your position in the bank?
- What does the Operational Risk mean to your organization as part of the Risk Management procedure?
- What are your formal responsibilities regarding risk taking?
- In your opinion, which are the factors connected with external fraud banking sector?
- In your opinion, which are the factors connected with cyber risk in banking sector?
- How do you grade your institution's ability to counter external fraud and cyber threats?
- How the cyber threat and external fraud influence as factors for a crisis in the banking industry with malfunction at the business continuity planning?
- Do you think that more attention should be given to the risk assessment before a risk decision is made? If so, Why?

4.8.1. How long have you been employed on your organization? What is your position in the bank?

	Working Years	Working Position
S1	10	Supervisor
SM1	20	Sub Department Manager
SO1	2.5	Customer Support officer
M1	20	Manager
S2	15	Supervisor

4.8.2. What does the Operational Risk mean to your organization as part of the Risk Management procedure?

In this question, all the respondents agreed that is highly important and vital to organizations as part of the Risk management procedure. Specifically, M1supports that "Risk is the main cause of uncertainty in any organization. Having in mind this, operational Risk management is very important for our organization, it is a key element, because without it, cannot define our objectives for the future. Operational risk management helps limit surprises and quantify the potential impact of business decisions. Effective operational risk management has as a result a well-run business and a desired reputation". Furthermore, S2 supports that "The economic uncertainty of the past few years effect how banks operate these days. Our bank has a renewed focus to manage risk, especially operational risk. Risk is the main cause of uncertainty in any organization. Thus, our bank increasingly focusses more on identifying risks and managing them before they even affect the business. In addition to this, Operational risk plays a key role in our organization Risk management process, provides us the ability to manage operational risk, to act more confidently on future business decisions. Further, it is an important part of our organization management because without it, cannot possibly define its objectives for the future".

4.8.3. What are your formal responsibilities regarding risk taking?

The five respondents agreed that the formal responsibilities regarding risk taking are: Report an incident, identified the risks, and decided the methods of assessment and monitoring. According SO1, the responsibilities that has is to "Make sure that my conduct does not breach any policies or compliant requirements and report such breaches, from colleagues or clients." Furthermore, M1 said that" is responsible for identifying and monitoring the risks in my own units and for ensuring that the control activities work. Ensure that these are reported to Operational Risk department, ensure that appropriate control measures are in place for managing those risks. Continually monitor the adequacy and effectiveness of all control measures and report".

4.8.4. In your opinion, which are the factors connected with external fraud banking sector?

The respondents of the interviews replied that the factors connected with external fraud banking sector are: Money laundering, banks data security and access sensitive information, execution of illicit transactions, Card copying, misrepresentation. Moreover, S2 mentioned also some other factors: Social – culture factors, lack of staff training.

4.8.5. In your opinion, which are the factors connected with cyber risk in banking sector?

In this question respondents replied that the factors connected with cyber risk are: Data security, Advance computer technologies, and insufficient staff training. According to SO1 "another factor connected with cyber risk are Internet crime, hacking, online shopping, and phishing".

4.8.6. How do you grade your institution's ability to counter external fraud and cyber threats?

Manager, Supervisors and Sub department manager grade their institutions ability to counter external fraud and cyber threats as highly able to prevent such threats. SO1 believes that the organization that is working needs improvement.

4.8.7. How the cyber threat and external fraud influence as factors for a crisis in the banking industry with malfunction at the business continuity planning?

The respondents of the interviews replied that cyber threat and external fraud influence as factors for a crisis in the banking industry with malfunction at the business continuity planning with Business disruption, can create financial losses, reduce clientele and affect the credibility and reputation of the business.

4.8.8. Do you think that more attention should be given to the risk assessment before a risk decision is made? If so, Why?

All the five respondents respond to this question positively. S1 argues that "Every decision should be examined thoroughly and all risks should be evaluated." SM1 said "yes, because risk assessment: create awareness of the risk, evaluate risk. According to M1" Determine if existing control measures are suitable or if more should be done, Meet legal requirements where applicable". Last S2 said "Yes, because it is a systematic method, assess the risk, considering what could go wrong, deciding on suitable control measures to prevent losses".

Chapter 5
Conclusion and recommendation

5.1. Conclusion

The aim of this study was to examine at providing more understanding of cyber risk and external fraud, with emphasizes in risk assessment. Risk assessment provides a comprehensive model that can be applied in identifying the methods through which cyber threat and fraud are committed, avoiding further risk activities occurring and providing guidelines of handling those events and acting against perpetrators.

Nowadays, Operational Crisis Management in the Banking Sector is one of the most crucial and everyday risks that banks dealing with and this is acceptable from everyone. According to Risk. Net (2017) the two most important operational risks for 2017 are Cyber threats and External Fraud. It is very crucial for all connecting direct or indirect to these risks to understand the factors connected to those risks and the impact on business continuity. In Conclusion, Cybercrime and external fraud are emerging as a challenge for security in the international banking sector.

5.1.1. First Research Question

People, Systems, processes and external events are factors that affect Operational risk of Cyber threats and External fraud in International banking. These factors apply to an organization's business environment and control is very important that the identified factors must be measurable to ensure that they can determine the level of risk. Therefore, it can be concluded that these factors are the pillars of operational risk, cyber threats and external fraud, which

should form an essential part of an operational risk management process. Especially, people (65%) and processes (58.3%) play a very important role as factors linked to the operational risk of banking sector.

5.1.2. Second Research Question

Business Continuity Planning is a key aspect of business continuity management, which contains business practices that offer focus and guidance on the decisions and actions required to prevent, mitigate, prepare, respond, and recover from a crisis (Shaw and Harrald, 2004). There is a significant relationship between Business Continuity Planning and External Fraud and Cyber Threats. Therefore, when a crisis occurs, either is a cyber thread or external fraud event and the business continuity planning is not effective or efficient can hurt the banks with various ways such as financial losses, affect the credibility and reputation.

5.1.3. Third Research Question

Risk assessment is one of the critical steps of the risk management. There is strong relationship between the Risk Assessment and external fraud and cyber threats. Therefore, Risk Assessment can be used to create appropriate policies and select techniques to implement them. Risk Assessment create awareness, evaluate a risk, through this procedure operational risk managers in banking sector can clarify if the existing controls of a risk event is suitable to deal with this risk.

5.2. Recommendations

- Banks should establish formal operational risk management structures
- Such structures will ensure the correct allocation of responsibilities to staff involved in managing operational risk.
- It is important to develop and implement training programs accordance to operational risk. This will improve the awareness of operational risk linked the bank
- All banks should investigate and implement a formal quantitative method to measure operational risk. This will ensure that all operational risks will be addressed in the form of control measures and techniques.

Bibliography

- Abraham, H. (2008). Bank runs: A risk mismanagement perspective: A Note. South African Journal of Business Management, Vol. 39, Issue 4, p. 63-65.
- ACFE, "Report to the Nation on Occupational Fraud and Abuse, (2010).The Association of Certified Fraud Examiners, Available From: www.acfe.com
- Acharyya, M. (2010). The role of operational risk and strategic risk in the enterprise risk management framework of financial services firms, Int. J. Services Sciences, Vol. 3, No. 1, a p.79–102.
- Ackerman, G. (2013). G-20 urged to treat cyber-attacks as threat to global economy,' Bloomberg, from www.bloomberg.com/news/2013-06-13/g-20-urged-to-treat-cyber-attacks-as-threat-to-economy.html, accessed 18 January 2014
- Adeoti, J. O. (2011), Automated Teller Machine (ATM) Frauds in Nigeria: The Way Out", Journal of Social Sciences, 21(1), pp 53-58.
- Adeyemo, K. A. (2012). Frauds in Nigerian Banks: Nature, Deep-Seated Causes, Aftermaths and Probable Remedies", Mediterranean Journal of Social Sciences, 3(2), pp 279-289.
- Aebi, V., Sabato, G., & Schmid, M. (2012). Risk management, corporate governance, and bank performance in the financial crisis", Journal of Banking & Finance, pp. 3213–3226.
- Ahmed I., Madawaki M.D.,Usman F.,(2014). Managing bank fraud and forgeries through effective control strategies. A Case study of Central bank of Nigeria,Combe Branch. International Journal of Business and Management Invention ISSN (Online): 2319 – 8028, ISSN (Print): 2319 – 801X.
- Albrecht, W. S., Albrecht, C. C., & Albrecht, C. O. (2004). Fraud and corporate executives: Agency, stewardship, and broken trust. Journal of Forensic Accounting, V, 109-130.
- Albrecht, W.S. (1996). Employee fraud. Internal Auditor, October, p. 26.

- Alexander, C. (2003). Operational risk: regulation, analysis and management. Harlow: Pearson Education
- Amel, D. F. and J. N. Liang (1992). The Relationship between Entry into Banking Markets and Changes in Legal Restrictions on Entry, Antitrust Bulletin, 37, 631–649.
- Anadarajan, A., & Kleinman, G. (2011). The impact of cognitive biases on fraudulent behaviour: the Leeson case. International Journal of Behavioural Accounting and Finance, 2 (1), 40-55.
- Andersen, L.B., Maberg, S., Hägerwzx, D., Næss M.B. & Tungland, M. (2012). The financial crisis in an operational risk management context – A review of causes and influencing factors, Reliability Engineering & System Safety, vol. 105, pp. 3-12.
- Apatachioae, A. (2014). New challenges of the management of banking risks, Procedia Economics and Finance, vol.15, pp. 1364-1373.
- Arachchilage, N. A. G., & Love, S. (2013). A game design framework for avoiding phishing attacks. Computers in Human Behavior, 29(3), 706 - 714.
- Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. Computers in Human Behavior, 38, 304-312.
- Ariffin, N. M. Archer, S. and Karim, R. A. A. (2009). Risks in Islamic banks: Evidence from empirical research. Journal of Banking Regulation; Vol. 10, Issue 2, p. 153-163.
- Ariss, R. T. and Sarieddine, Y. (2007). Challenges in implementing capital adequacy guidelines to Islamic banks. Journal of Banking Regulation; Vol. 9, Issue 1, p. 46-59.
- Arora, Diksha and Agarwal Ravi, (2009). Banking Risk Management in India and RBI Supervision, pp. 5-22, Electronic copy available from: http://ssrn.com/abstract=1446264
- Assessment - Practices of Leading Organizations, A Supplement to GAO's (May 1998). Executive Guide on Information Security Management [Online]. Available at http://www.gao.gov/special.pubs/ai00033.pdf [accessed date 30 Mar 2008]

- Bank for International Settlements (2003). Sound Practices for the Management and Supervision of Operational Risk, Risk Management Group of the Basel Committee on Banking Supervision (February).
- Bank of Pakistan, (2003).Risk management guidance for commercial banks & DFIs‟
- Barakat, A. & Hussainey, K. (2013). Bank governance, regulation, supervision, and risk reporting: Evidence from operational risk disclosures in European banks, International Review of Financial Analysis, pp. 254–273.
- Barlow, Lyde and Gilbert. Scott, A. (2000). Risk management for accountants. London: ABG Professional Information
- Barnes, R.W., (1995). The value of quality education to banks and bankers. The Journal of Indian Institute of Bankers, 66(3) pp 55-59.
- Basel Committee on Banking Supervision (1996). Amendment to the Capital Accord to incorporate market risks, Basel January 1996
- Basel committee on banking supervision (2001). Operational risk-supervisory guidelines for the advanced measurement approach‟, Banks for International Settlements, Basel.
- Basel Committee on Banking Supervision (2001a). The New Basel Capital Accord, Basel January 2001.
- Basel Committee on Banking Supervision (2001b). Results of the Second Quantitative Impact Study, Basel November 2001.
- Basel Committee on Banking Supervision (2002). Results of Quantitative Impact Study 2.5, Basel June 2002.
- Basel Committee on Banking Supervision (2003a). The New Basel Capital Accord, Basel April 2003.
- Basel Committee on Banking Supervision (2006). International Convergence of Capital Measurement and Capital Standards: A Revised Framework, Comprehensive Version. Switzerland: Bank for International Settlements.

- Basel Committee on Banking Supervision (2008). Observed range of practice in key elements of Advanced Measurement Approaches (AMA), Banks for International Settlements, Basel.
- Basel Committee on Banking Supervision (BCBS), (2011). Principles for the sound Management of Operational Risk. Bank for International Settlements.
- Basel Committee on Banking Supervision (BCBS), (2003). Sound Practices for the Management and Supervision of Operational Risk.
- Basel Committee on Banking Supervision (BCBS), (2006). International Convergence of Capital Measurement and Capital Standards A Revised Framework Comprehensive Version.
- Basel Committee on Banking Supervision (BCBS), (2003). Sound Practices for the Management and Supervision of Operational Risk, Bank for International Settlements.
- Basel Committee on Banking Supervision (January 2001). Operational Risk, Consultative Document", Supporting Document to the New Basel Capital Accord.
- Basel Committee on Banking Supervision (June 2006). International Convergence of Capital.
- Basel Committee on Banking Supervision (June 2006). International Convergence of Capital Measurement and Capital Standards, Banks for International Settlements, Basel.
- Basel Committee on Banking Supervision, (1998c). Risk management for electronic banking and electronic money activities. , Banks for International Settlements, Basel.
- Basel Committee on Banking Supervision, (2004). International Convergence of Capital Measurement and Capital Standards; Bank for International Settlements Press & communication; Basel, Switzerland, June 2004.
- Basel Committee on Banking Supervision, (2003). Sound Practices for the Management and Supervision of Operational Risk; Bank for International Settlements Press & communication; Basel, Switzerland, February 2003.
- Basel II. (2001a). Operational risk. Consultative document. Retrieved from: https://www.bis.org/publ/bcbsca07.pdf

- Basel II. (2001b). Working paper on the regulatory treatment of operational risk. Retrieved from: http://www.bis.org/publ/bcbs wp8.pdf
- BCBS (2006). International Convergence of Capital Measurement and Capital Standards, A Revised Framework, Comprehensive Version. Basel Committee on Banking Supervision, Bank for International Settlement, Basel.
- Beans, K. M. (2010). Risk Management after the Crisis, the RMA Journal, pp. 20-25.
- Berger, A. Klapper, L. and Turk-Ariss, R. (2009). Bank Competition and Financial Stability. Journal of Financial Services Research; Vol. 35, Issue 2, p. 99-118.
- Berger, A. N. and D. B. Humphrey (1992). Megamergers in Banking and the Use of Cost Efficiency as an Antitrust Defense, Antitrust Bulletin, 37, 541–600.
- Berger, A. N. and D. B. Humphrey (1997). Efficiency of Financial Institutions: International Survey and Directions for Future Research, European Journal of Operational Research, 98(2), 175–212.
- Berger, A. N. and L. J. Mester (1997). Inside the Black Box: What Explains Differences in the Efficiencies of Financial Institutions? Journal of Banking and Finance, 21, 895–947.
- Berger, A. N. and R. DeYoung (2001). The Effect of Geographic Expansion on Bank Efficiency, Journal of Financial Service Research, 19(2–3), 163–184.
- Berger, A. N., R. S. Demsetz, and P. E. Strahan (1999). The Consolidation of the Financial Services Industry: Cause, Consequences and Implications for the Future, Journal of Banking and Finance, 23(2–4), 175–212.
- Bhasin, M. (2007). Mitigating cyber threats to banking industry. The chartered accountant, 55(10), 1618 -1624
- Bhasin, M. (2007). The Bank Internal Auditor as Fraud Buster. The ICFAI Journal of Audit Practice, Vol. 4, No.1, January.
- Biener, C., Eling, M., Wirfs, J.H. (2015). Insurability of cyber risk: An empirical analysis. Geneva. Pap. Risk. Ins. **40**, 131–158.

- Bierstaker, J. Brody, R.G. and Pacini, C. (2006). Accountants‟ perception regarding fraud detection and prevention methods. Managerial Auditing Journal, Vol. 21, No. 5, pp 520-535.
- Black, W. K. (2005b). The best way to rob a bank is to own one: How corporate executives and politicians looted the S&L industry. Austin, TX: University of Texas Press.
- Bologna, J. (1993). Handbook on Corporate Fraud, Butterworth-Heinemann, Stoneham, MA, pp. 54-62.
- "Business Continuity Planning", accessed on Dec 2011, http://www.bankinfosecurity.com/ten-stepsto-effective-business-continuity-plan-a-186/p-2 5. "Difference between Disaster recovery and Business Continuity", accessed on Dec 2011
- Cagan, P. (2001). Standard operating procedures, Erisk.com
- Cagan, P. (2009). Managing operational risk through the credit crisis, The Journal of Compliance Risk and Opportunity, vol.3, no.2, p.19-26.
- Calderon, T. and Green, B.P. (1994). Internal fraud leaves its mark: here's how to spot, trace and prevent it. National Public Accountant, Vol. 39, August, p. 17.
- Calderon, T. and Green, B.P. (1994). Internal fraud leaves its mark: here's how to spot, trace and prevent it. National Public Accountant, Vol. 39, August, p. 17
- Canhoto, A. I., & Backhouse, J. (2007). Profiling under conditions of ambiguity - an application in the financial services industry. Journal of Retailing and Consumer Services, 14, 408-419
- Carey, A. (2001). Effective risk management in financial institutions: the Turnbull approach. Balance Sheet; Vol. 9, Issue 3, p. 24-27.
- Carroll, J. J. (1998). Evaluations of Risk: Do Organizational or Individual Biases Prevail? Academy of Management Executive; Vol. 12, Issue 4, p. 129-130.
- Carter, A. & Chinyio, E. (2012). Effectiveness of risk management: barriers and Solutions, Int. J. Project Organization and Management, vol. 4, no. 4, pp.368-378.

- Cebula, J.J., Young, L.R. (2010). A Taxonomy of Operational Cyber Security Risks, Software Engineering Institute, Carnegie Mellon University.
- Chartered Institute of Management Accountants (2008). Fraud Risk Management: A guide to good practices. Available From: http://www1.cimaglobal.com/Documents/ImportedDocuments/cid_techguide_fraud_risk_management_feb09.pdf.pdf [Accessed on 30 April 2012]
- Chatterjee, P. (2007). Troubles light up in the dawn of Basel II. Banker; Vol. 157, Issue 982, p. 12.
- Chavez-Demoulin, P. Embrechts & j. Neŝlehová (2006). Quantitative models for operational risk: Extremes, dependence and aggregation, Journal of Banking and Finance, 30, pp. 2635-2658
- Chernobai, A., Jorion, P., & Yu, F. (2011). The Determinants of Operational Risk in U.S. Financial institutions, Journal of financial and quantitative analysis, vol. 46, no. 6, pp. 1683–1725.
- Choo, K. K. R. (2011). The cyber threat landscape: Challenges and future research directions. Computers & Security, 30(8), 719-731. Center for Internet Security: CIS Security Controls.
- Cleden, D., (2009). Managing project uncertainty. Abingdon: Ashgate Publishing Group.
- Cloward, R. A., & Ohlin, L. E. (1966). Delinquency and opportunity. New York: Free Press.
- Coleman R and Cruz M (1999). Operational Risk Measurement and Pricing. Derivatives Week, Vol. 8, No. 30, (July 26): 5–6.
- Collier, M.P. (2009). Fundamentals of Risk management for Accountants and Managers. Tools and techniques, Elsvier Ltd.
- Commercial Angles Newsletter. (2001). Fraud Prevention. July, available www.commercialangles.com/articles/fraud_control.htm
- Committee on Payments and Market Infrastructures and International Organization of Securities Commissions (2016). Guidance on cyber resilience for financial market infrastructures, June.

- Comptroller of the currency, (1994). Risk Management of financial derivatives: Comptroller's Handbook. Washington: Administrator of National Banks, October.
- Consultative Document on Operational Risk, Basel Committee on Banking Supervision, January (2001). Available From: https://www. bis.org/publ/bcbsca07.pdf
- Coombs, W.T. (2007). Crisis Management and Communications. Retrieved 1 March 2015 from http://www.facoltaspes.unimi.it/files/ ITA /COM/Crisis Management and Communications.pdf
- Cooper, D., Grey, S., Raymond, G. & Walker, P. (2005). Project Risk management guideline: Managing risk in the large projects and complex procurements. Hoboken, NJ: J. Wiley.
- Cooper, D., Grey, S., Raymond, G. & Walker, P., (2005). Project Risk management guideline: Managing risk in the large projects and complex procurements. Hoboken, NJ: J. Wiley.
- Cooper, D., Grey, S., Raymond, G., and Walker, P., (2005). Project Risk Management Guidelines: Managing Risk in Large Projects and Complex Procurements. Chichester: John Wiley & Sons, Ltd
- Cornia, A., Dressel, K. & Pfeil, P.(2014). Risk cultures and dominant approaches towards disasters in seven European countries, Journal of Risk Research, pp. 1-17.
- Costello, B. (1997). On the logical adequacy of cultural transmission theories. Theoretical Criminology, 1 (4), 403-428.
- Council for Registered Ethical Security Testers (2017). A guide for running an effective penetration testing program.
- Cressey, D. (1973). Other People's Money: A study in the social psychology of embezzlement. New Jersey: Patterson Smith Publishing Corporation.
- Cressey, D. (1953). Others people's money: a study in the social psychology of embezzlement. Glencoe, IL: Free Press.
- Crouhy M. & Mark R., (2000). Operational Risk in the professional's handbook of financial risk management, edited by M. Lore & L. Borodovsky. Oxford: Butterworth Heineman: 342-365.

- Crouhy, M., Galai,D.& Mark R. (1998). Key steps in building Consistent operational risk measurement and management, in operational risk and financial institution, edited by Robert Jameson. London: Risk Books: 45-62
- Cruz M., Coleman R. and Gerry S. (1998). Modeling and Measuring Operational Risk. Journal of Risk, Vol. 1, No. 1: 63–72.
- Cruz MG. (2002). Modeling, Measuring and Hedging Operational Risk, John Wiley & Sons, Ltd.
- Culbertson, D. (2004). IT risk: A new challenge for community bank", Bank News.
- Cyber Crime Overview. (2008). Available from: http:// cybercrimeindo.blogspot.com [accessed on 25 April 2010].
- Cyber Crimes. April (2008). Available from: http://theviewspaper.net/cyber_crimes [accessed on 25April 2010].
- Cyber Forensics. (2008). Available from: http://www.santoshraut.com/forensic/cybercrime.htm [accessed on 25 April 2010].
- Darnall, R. and Preston, J.M. (2010). Project Management from Simple to Complex. Flat World Knowledge, Inc.
- Das, S. R. (2007). Basel II: Correlation Related Issues. Journal of Financial Services Research; Vol. 32, Issue 1/2, p. 17-38.
- Davies J. Fairless M., Libart S. Love J. O'brien D., Slater P., & Shepheard-Washington T., (1998). Defining and aggregating operations risk information in operational risk and financial institutions, edited by Robert Jameson. London: Risk Books: 63-80.
- Davies J. Fairless M. Libart S. Love J. O'brien D., Slater P., & Shepheard-Washington T. (1998). Defining and aggregating operations risk information in operational risk and financial institutions, edited by Robert Jameson. London: Risk Books: 63-80.
- Davis, E. (2006). The advanced measurement approach to operational risk. London: Risk Books
- Davis, E.L. (2005). Operational risk: practical approaches to implementation. London: Risk Books

- Day, R. (2010). Applying the Fraud Triangle Model to the Global Credit Crisis. Retrieved from Nordicum-Mediterraneum (Icelandic E-Journal of Nordic and Mediterranean Studies) 5(1). Available From: http://nome.unak.is/nm/5-1/12-reflection-on-the-economic-crisis-/236-applying-the-fraud-triangle-model-to-the-global-credit-crisis [Accessed on July 1, 2011].
- De Fontnouvelle, P. DeJesus-RueffJohn, V., Jordan, J. and Rosengren, E., (2003). Using loss data to quantify operational risk. Federal Reserve, Bank of Boston.
- Deloitte, (2016). Global Risk Management Survey, 10th edition.
- Department of Financial Services of New York State (2017). Cyber-security requirements for financial services companies.
- Donahoe T.C. (1999).Role playing. Some operational risk groups are struggling to make their remit clear: Operational risk special report. Risk, July: 3
- Donahoe T.C. (1999).Role playing. Some operational risk groups are struggling to make their remit clear: Operational risk special report. Risk, July: 3.
- Dowd, K. (1998). Beyond value at risk: the new science of risk management. Chichester: Wiley. (Wiley Series in Frontiers in Finance).
- Durkheim, E. (1964). The Division of labor of society. New York: Free Press.
- Ebnöther, S. Vanini, P. McNeil, A. and Antolinez, P. (2003). Operational risk: a practitioner's view. Journal of Risk; Vol. 5, Issue 3, p. 1-15.
- Ebnother, S., P. Vanini, A. McNeil, and Antolinez, P. (2003). Operational Risk: A Practicioner's View, Journal of Risk, 5.
- Ekpechi, A.O. (2006). Fraud and Forgeries in Banks, Types, and Prevention". Being paper presented at National Seminar on bank audit, organized by ICAN.
- Embrechts P, McNeil A and Rudiger F (2005). Quantitative Risk Management, Techniques and Tools. Princeton Series in Finance.
- Esterhuysen, J. (2010). The effect of stressed economic conditions on operational risk loss distributions", SAJEMS NS, vol. 13, no 4.pp.476-492

- European Commission (2012). Special Eurobarometer 390 Cyber Security. Retrieved 9 December 2013 from http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf
- Fadipe-Joseph, O. A., & Titiloye, E. O. (2012). Application of Continued Fractions in controlling Bank Fraud, International Journal of Business and Social Science, 3(9), pp 210-213.
- Falkena, H.G. & Kok, W.J. (1999). Essays on Financial Risk Management, 80(06), February: 13.
- FFFS (2014). Finansinspektionen's Regulations and General Guidelines regarding the management of operational risks.
- Fheili, M.I. (2011). Information technology at the forefront of operational risk: banks are at a greater risk, The Journal of Operating risk, vol.6, no.2, pp. 47-67.
- Financial and Management accounting committee (1999). Enhancing shareholder wealth by better managing business risk, edited by Price water house Coopers. New York.
- Financial Stability Board (2014). Guidance on supervisory interaction with financial institutions on risk culture: A framework for assessing risk culture.
- Finau, G., Samuwai, J. & Prasad, A. (2013). Cybercrime and its implications to the pacific. The Accountant: The journal of the Fiji Institute of Accountants.
- Fournier, E. De Cordova, P. G. James, B. Miles, A. Crompton, S. Faith, J. Gleeson, S. Blackmore, V. Evans, R. Siskey, K. De Verneuil, V. Nishiyama, K. Seem, A. Ikeda, M. Ozawa, J. Stender, N. Zhou, L. L. Zeng, Y. Elliott, G. and Irani, V. (2008). Regulatory Capital Is Broken. International Financial Law Review; Vol. 27, Issue 12, p. 1.
- Fraud and Abuse, (2012). Available From: http//www.efenet.com/summary.
- Ganegoda, A. & Evans, J. (2014). A framework to manage the measurable, immeasurable and the unidentifiable financial risk", Australian Journal of Management, pp. 5-34.

- Ganesh, A. and Raghurama, A. (2008). Status of training evaluation in commercial bank- a case Study. Journal of Social Sciences and Management Sciences, Vol. XXXVII, No.2, Sept, pp 137-58.
- Gaylord, M.S. and Galliher, J.F. (1988). The Criminology of Edwin Sutherland. New Brunswick, NJ: Transaction Books
- Goldman, Sachs & Co and Swiss Bank Corporation (1998). The practice of risk management. Implementing processes for managing firm wide market risk, edited by E.R. Corrigan. London: Euro money Books.
- Gould, F.E, and Joyce, N.E (2002). Construction project management. Upper Saddle River: Prentice Hall
- Goyal A.K. (2010). Risk Management in Indian Banks: Some Emerging Issues. Int. Eco. J. Res., 102-109.
- Goyal A.K. (2010). Risk Management in Indian Banks: Some Emerging Issues. Int. Eco. J. Res., 102-109
- Goyal A.K. (2010). Risk Management in Indian Banks: Some Emerging Issues. Int. Eco. J. Res., 102-109.
- Gracie, A. (2014). Managing cyber-risk – the global banking perspective, 10 June.
- Greenbaum, S. I., & Thakor, A. V. (2007). Contemporary financial intermediation (2nd Ed.). London: Elsevier Academic Press.
- Grody, A. D., Harmantzis, F. C. and Kaple, G. J. (2005). Operational Risk and Reference Data: Exploring Costs, Capital Requirements and Risk Mitigation, Stevens Institute of Technology, Hoboken, NJ.
- Gunther, H. and Christian, W. (2005). Determinants of Operational Risk Reporting in the Banking Industry"
- Hackmageddon.com (2013). 'Cyber-attack statistics'

Available From www.hackmageddon.com/2013-cyber-attacks-statistics/, accessed 1 May 2014.

- Hamberg, M. (2000). Risk, uncertainty & profitability: an accounting-based study of industrial firm's financial performance. PhD Thesis, Uppsala University. Perth: Uppsala University.

- Harmantzis, F. (2002). Operational Risk Management in Financial Services and the New Basel Accord, working paper, Stevens Institute of Technology.
- Harris and William (2004). The Two Faces of the Transgender Fraudster Who Made Thousands of Pounds in Scams Posing as Both Sexes.
- Hartmann-Wendels, T., Mählmann, T., & Versen, T. (2009). Determinants of banks' risk exposure to new account fraud - Evidence from Germany. Journal of Banking and Finance, 33, 347-357.
- Harvard Business Review Analytic Services (2013). Meeting the Cyber Risk Challenge, Boston, MA: Harvard Business School Publishing
- Haselkorn D., Khaykin I. & Eaton R., (2015). Risk identification: What have banks been missing? Marsh & Mclennan companies.
- Haugen, S. and Selin J.R. (1999). Identifying and controlling computer crime and employee fraud. Journal
- Healey, J. (2013). A Fierce Domain: Conflict in Cyberspace, 1986 to 2012, Vienna, VA: Cyber Conflict Studies Association.
- Helbok, G and Wagner, H. (2006). Determinants of operational risk reporting in the banking industry, Journal of Risk, July 11.
- Herring, R. J. (2007). The Rocky Road to Implementation of Basel II in the United States. Atlantic Economic Journal; Vol. 35, Issue 4, p. 411-429.
- Heru, S., Na (2005). Analyzing and Scaling Operational Risk Loss Data, Erasmus University Rotterdam, Netherlands. Master's Thesis.
- Hoffman D.G., (1998). New trends in operational risk measurement and management in operational risk and financial institutions, edited by Robert Jameson. London: Risk Books: 29-42.
- Hoffman, D. (2002). Managing operational risk: 20 firm wide best practice strategies. New York: Jonn Wiley and Sons. (Wiley Finance Series).
- Hollinger, R. C., & Clark, J. P. (1983). Deterrence in the workplace: Perceived certainty, perceived severity and employee theft. Social Forces, 62, 398-418.
- Holton, C. (2009). Identifying disgruntled employee systems fraud risk through text mining: A simple solution for a multi-billion dollar problem. Decision Support Systems, 46 (4), 853-864.

- Hong Kong Monetary Authority (2015). Cyber-security risk management, September.
- Hopkin P., (2010). Fundamentals of Risk Management: Understanding, evaluating and implementing effective risk management. Kogan Page Limited
- Hopkin P., (2010). Fundamentals of Risk Management: Understanding, evaluating and implementing effective risk management. Kogan Page Limited
- Hopkin P., (2010). Fundamentals of Risk Management: Understanding, evaluating and implementing effective risk management. Kogan Page Limited
- Hopkin P., (2010). Fundamentals of Risk Management: Understanding, evaluating and implementing effective risk management. Kogan Page Limited
- Hopkin P., (2010). Fundamentals of Risk Management: Understanding, evaluating and implementing effective risk management. Kogan Page Limited
- Hopkin P. (2010). Fundamentals of Risk Management: Understanding, evaluating and implementing effective risk management. Kogan Page Limited
- Hopkin P. (2010). Fundamentals of Risk Management: Understanding, evaluating and implementing effective risk management. Kogan Page Limited
- Hopkin P. (2010). Fundamentals of Risk Management: Understanding, evaluating and implementing effective risk management. Kogan Page Limited
- Hopkin P. (2010). Fundamentals of Risk Management: Understanding, evaluating and implementing effective risk management. Kogan Page Limited
- Howell, J. (2014). Board Reporting Trends and Best Practices in the Digital Age", Financial Executive, pp. 32-36.

- Huang, C. J. and Tsu-Tan Fu (2001). Uncertainty, Risk Premium and Productivity in the Taiwan Banking Industry, Working Paper, Vanderbilt University.
- Hughes, J. P. and L. J. Mester (1993). A Quality and Risk-Adjusted Cost Function for Banks: Evidence on the 'Too-Big-To-Fail' Doctrine, The Journal of Productivity Analysis, 4, 293–315.
- Hughes, J. P. and L. J. Mester (1998). Bank Capitalization and Cost: Evidence of Scale Economies in Risk Management and Signaling, Review of Economics and Statistics, 80(2), 314–325.
- Hughes, J. P., L. J. Mester, and Choon-Geol Moon (2001). Are Scale Economies in Banking Elusive or Illusive? Evidence Obtained by Incorporating Capital Structure and Risk- Taking into Models of Bank Production, Journal of Banking and Finance, 25, 2169– 2208.
- Hughes, J. P., W. Lang, L. J. Mester, and Choon-Geol Moon (1996). Efficient Banking under Interstate Branching, Journal of Money, Credit, and Banking, 28, 1045–1071.
- Hunton, P. (2009). The growing phenomenon of crime and the Internet: A cybercrime execution and analysis model. Computer Law & Security Review, 25(6), 528 - 535.
- Idolor, E. J. (2010). Bank Fraud in Nigeria: Underlying Causes, Effects and Possible Remedies, African Journal of Accounting, Economics, Finance and Banking Research, 6(6), pp 62.
- Idowu, A. (2009). An Assessment of Fraud and its Management in Nigeria Commercial Banks. European Journal of Social Sciences. 10, (4), 628-640.
- Idowu, I. (2009). An Assessment of Fraud and its Management in Nigeria Commercial Banks, European Journal of Social Sciences, 10(4), pp 628-640. Association of Certified Fraud Examiners (1999), Report on the Nation Occupational.
- Ingley, C. & Walt, N. (2008). Risk Management and Board Effectiveness", Int. Studies of Mgt. & Org., vol. 38, no. 3, pp. 43–70.
- ISO 17776, (2000). Petroleum and natural gas industries-Offshore production installations-Guidelines on tools and techniques for hazard

identification and risk assessment. First edition. ISO-International Organization for Standardization

- ISO/IEC 15504 (2003). Information Technology – Process Assessment: part1 - Part5; ISO; Geneva, Switzerland, 2003.
- Jobst AA (2007). Operational Risk — the Sting is still in the Tail but the Poison Depends on the Dose. IMF Working paper 07/239, International Monetary Fund.
- Jobst AA (2007). Operational Risk — the Sting is still in the Tail but the Poison Depends on the Dose. IMF Working paper 07/239, International Monetary Fund.
- Jobst AA, (2007). The Regulation of Operational Risk under the New Basel Capital Accord - Critical Issues. International Journal of Banking Law and Regulation, Vol. 21, No. 5: 249–73.
- Jobst AA, (2007). The Regulation of Operational Risk under the New Basel Capital Accord - Critical Issues. International Journal of Banking Law and Regulation, Vol. 21, No. 5: 249–73.
- Jobst, A.A. (2010). The credit crisis and operational risk – implications for practitioners and regulators", The Journal of Operational Risk, vol. 5, no. 2, pp. 43–62.
- Jongh, E., Jongh, D.R., Jongh, R. & Vuuren, G. (2013). A review of operational risk in banks and its role in the financial crisis", SAJEMS, vol.16, no.4, pp.364-382.
- Kaiser, T. (2006). An introduction to operational risk: a practitioner guide. London: Risk Books
- Kaplan, J, T Bailey, D O'Halloran, A Marcus and C Rezek (2015). Beyond cybersecurity, Wiley.
- Kaplan, S. & Garrick, B. J. (2006). On The Quantitative Definition of Risk, Risk Analysis, pp. 11-27.
- Katz I.D. (1995). Financial Risk Manager. London: Euro money Books.
- Katz I.D. (1995). Financial Risk Manager. London: Euro money Books.
- Keefe, B. & Pfleiderer, A. (2012). Basel III: What It Means for the Global Banking System, Banking and finance law review, pp. 407-426.

- Khan, T. and Ahmed, H. (2003). An analysis of issues in Islamic financial industry.
- Khanna, A. and Arora, B. (2009). A study to investigate the reasons for bank frauds and the implementation of preventive security controls in Indian banking industry, International Journal of Business Science and Applied Management, Vol. 4, No. 3.
- Kim, Y. & Vonortas, N. S. (2014). Managing risk in the formative years: Evidence from young enterprises in Europe", Risk and Uncertainty Management in Technological Innovation, vol. 34, no. 8, pp. 454-465.
- KING Jack L. (2001). Operational Risk; Wiley Finance, Series, New York.
- King JL (2001). Operational Risk: Measuring and Modelling. John Wiley & Sons, New York
- Kingsley S. Rolland A. Tinney A., & Holmes P. (1998). Operational risk and financial institutions: Getting started in operational risk and financial institutions, edited by Robert Jameson. London: Risk Books: 1-27.
- Kizza J.M. (2005). Computer network security. Springer Science & Business Media, Inc.
- KPMG (1999). Banking news: the Basel committee policy papers. Special issue of KPMG financial business unit, January:3-16.
- Kwan, S. and Eisenbeis, R. A. (1997) Bank Risk, Capitalization, and Operating Efficiency, Journal of Financial Services Research 12:2/3 117±131 Kluwer Academic Publishers.
- Lam J., (2014) Enterprise risk management: from incentives to controls, second edition. Published by John Wiley & Sons, Inc.
- Lang, W. and Nayda, W. (2008). Is Advanced Credit Risk Management Worth the Plunge? RMA Journal; Vol. 90, Issue 8, p. 35-41.
- Larrow, R.A. (2008). Operational risk, Journal of Banking and Finance, vol. 32, pp.870 – 879.
- Laub, J.H., (2006). Edwin H. Sutherland and the Michael-Adler Report: Searching for the Soul of Criminology Seventy years later. Criminology, 44(2), 235-464

- Lautenschläger, S (2017). Cyber resilience – A banking supervisor's view, Statement at the high-level meeting on cyber resilience, 19 June.
- Leippold, M., and Vanini, P. (2003). The quantification of operational risk, Journal of Risk 8, November 3, p. 1.
- Leong, K. S. (1996). The Right Approach: Value at Risk. Risk Special Supplement; June 1996, p. 14.
- Lester, A. (2007). Project management, planning and control, 5th edition. Oxford: Elsevier Ltd.
- Loader, D. (2006). Operations risk: managing a key component of operational risk. Oxford: Elsevier. (Elsevier Finance Series).
- Machiraju, H.R (2008). Modern Commercial banking, 2nd ed., New Delhi: New Age International.
- Makarov, M. (2006). Extreme Value Theory and High Quantile Convergence, Journal of Operational Risk, Vol.1, No. 2.
- Manic, I. (2007). Mathematical Models for Estimation of Operational Risk and Risk Management, Master's Thesis.
- Manic, I. (2007). Mathematical Models for Estimation of Operational Risk and Risk Management, Master's Thesis.
- Marsh, (2013), Cyber Risk Survey 2013, from www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/techniker/risikomanagement/partner/Partnerbeitrag_Marsh_Cyber-Risk_Survey.pdf?__blob=publicationFile, accessed 16 December 2013.
- Martinez-Sanchez J.F., Martinez – Palacios M.T. & Venegas –Martinez F., (2016). An analysis on operational risk in international banking: a Bayesian approach (2007-2011). Estudios Gerenciales 32 (2016) 208–220.
- Mayland P.F. (1993). Bank operating credit risk assessing and controlling credit risk in bank operating services. United States of America: Probus Publishing.
- McAfee (2013). The economic impact of cybercrime and cyber espionage' Available from: www.mcafee.com/sg/resources/reports/rp-economic-impact-cybercrime.pdf, accesses 9 January 2014.

- McAleer, M., Jimenez-Martind, J.A. & Perez-Amaralda, T. (2013). Has the Basel Accord improved risk management during the global financial crisis, Econometric, North American Journal of Economics and Finance, vol. 26, pp. 250– 265.
- McLaughin, J. (2013). Operational Risk Management Is Critical to Bank Success", The RMA Journal, pp.56-59.
- McLaughin, S. (2008). Challenges for 2008 and Beyond. RMA Journal; Vol. 90, Issue 9, p. 20-21.
- Measurement and Capital Standards, Banks for International Settlements, Basel.
- Measurement and Capital Standards, Banks for International Settlements, Basel.
- Mee, P and Morgan J. (2017). Deploying a cyber risk strategy: Five key moves beyond regulatory compliance, Oliver Wyman.
- Merton, R.K. (1938). Social Structure and Anomie. American Sociological Review, October, 672-82.
- Merton, R.K. (1957). Social Theory and Social Structure. Michigan Law Review, Chp.66, Sect.1529, 131-160.
- Mignola, G. and Ugoccioni R. (2005). Tests of Extreme Value Theory, Operational Risk, Vol. 6, Issue 10.
- Mignola, G. and Ugoccioni, R. (2006). Sources of Uncertainty in Modeling Operational Risk Losses, Journal of Operational Risk, Vol. 1, No. 2 (summer).
- Moody, M. (2010). ERM & ISO 31000, Rough Notes, vol. 153, no.3. pp. 80-81.
- Moore R. (2005). Cybercrime: Investigating High-Technology Computer Crime. Anderson Publishing: Cleveland, Mississippi.
- Moosa I. (2007). Operational Risk: A Survey, Financial Markets, Institutions & Instruments, Vol. 16, No. 4, pp. 167-200
- Moosa, I., A. (2007). Operational Risk Management. 1st ed., New York: Palgrave Macmillan.
- Mori T., Hiwatashi, J. and Ide K. (2000). Measuring Operational Risk in Japanese Major Banks, July 14, Bank of Japan Working Paper Series.

- Moscadelli, M. (2004). The Modelling of Operational Risk: Experience with the Data Collected by the Basel Committee, Discussion paper.
- Mukhopadhyay, A., Saha, D., Mahanti, A. and Chakrabarti, B. B. (2005), "Insurance for Cyber-Risk: A Utility Model," Decision 32(1): 153–169.
- Mulbert, P. & Wilhelm, A. (2011). Reforms of EU Banking and Securities Regulation after the Financial Crisis, Banking and Finance law review, pp. 187-231.
- Murphy D. S., & Robinson M. B. (2008). The maximizer: Clarifying Merton's theories of anomie and strain. Theoretical Criminology, 12 (4), 501-521.
- Mustaine E. E., & Tewksbury, R. (2002). Workplace theft: An analysis of student-employee offenders and job attributes. American Journal of Criminal Justice, 27 (1), 111-127.
- Nash T. (2003). Risk management: helping directors to identify and control business risks effectively. London: Director Publications (published for the Institute of Directors and AXA Insurance).
- National Bank of Ethiopia (2010). Commercial banks risk management guidelines.
- O'Hehir, M. 2007. What is a business continuity planning (BCP) strategy IN: Hiles, A. (ed) The Definitive Handbook Of Business Continuity Management. Second Edition, England: John Wiley & Sons Ltd, pp. 27-45.
- Olorunsegun, S. (2010). The Impact of Electronic Banking in Nigeria Banking System (Critical Appraisal of Unity Bank Plc), A Master Degree Dissertation submitted to Ladoke Akintola University of Technology, Ogbomoso, Oyo State, Nigeria.
- Omachonu, J & Ndiulor T. (1998). Banks Fraud Shrinks In Number, Balloons in Loot, The Guardian Newspaper, July 15, Lagos.
- Omar, N. B., & Mohamad Din, H. F. (2010). Fraud diamond risk indicator: An assessment of its importance and usage. International Conference on Science and Social Research (pp. 607-612). Kuala Lampur, Malaysia: IEEE
- Ong, M. 2007. The Basel Handbook: A guide for financial practitioners. 2nd Edition. Published by Risk Books Incisive Financial Publishing Ltd. London

- Onkagba, J.O. (1993). Auditing Computerization Information System: A Growing Audit Challenge. The Nigerian Accountant, Lagos, Published by ICA|N, Jan/Mar.
- Osborne A. (2012). Risk management made Easy. Andy Osborne and Ventus Publishing Aps. ISBN 978-87-7681-984-2.
- Paletta D. (2004). Basel II Banks' Monitoring Of Risk Ratings Said Lacking. American Banker; Vol. 169, Issue 98, p. 3.
- Panjer H (2006). Operational Risk: Modeling Analytics. Wiley.
- Passas N. (1990). Anomie and corporate deviance. Crime, Law and Social Change, 14 (2), 157-178.
- Passas, N. (1999). Continuities in the anomie tradition. In F. Adler, & W. Laufer (Eds.). The legacy of anomie theory. New York: Transaction Publishers.
- Perry J. (1986). Risk management – an approach for project managers. Butterworth & Co. Vol. 4, pp. 211-216.
- Peters G. and Terauds V. (2006). Quantifying Bank Operational Risk. Supplementary report.
- Picket, K. H. S. (2013). The essential guide to internal auditing. West Sussex: A John Wiley & Sons
- PMI (Project Management Institute) (2004). A guide to the project management body of knowledge: PMBOK. 3rd edition. Pennsylvania: Project Management Institute, Inc.
- PMI (Project Management Institute) (2004). A guide to the project management body of knowledge: PMBOK. 3rd edition. Pennsylvania: Project Management Institute, Inc.
- Porter D. (2003). Insider fraud: Spotting the wolf in sheep's clothing. Computer Fraud & Security, 4, 12-15.
- Potter E. J. (2002) Customer authentication: The evolution of signature verification in financial institutions. Journal of Economic Crime Management, 1 (1).
- Potts K. (2008). Construction cost management, learning from case studies. Abingdon: Taylor Francis.

- Power M. (2005).The invention of operational risk. Review of International Political Economy, October 2005: 577–599.
- Power M. (2005). The Invention of Operational Risk, Review of International Political Economy 12, 577-599.
- Power M. (2005). The invention of operational risk, Review of the International Political Economy, vol.12, no.4, pp.577-599.
- Power M. (2003). The invention of operational risk.
- PWC (2016). Cyber security and Business Continuity Management. Available from: http://www.epicc.org/uploadfiles/documents/PwC%20-%20Cyber%20Security%20and%20Business%20Continuity%20Management.pdf
- Rachlin C. (1998). Operational risk in retail banking: Promoting and embedding risk awareness across diverse banking groups in operational risk and financial institutions, edited by Robert Jameson. London: Risk Books: 113-126.
- Raghavan, R. S. (2003). Risk management in banks.
- Reuvid, J. (2007). Managing business risk: a practical guide to protecting your business. 4th ed. London: Kogan Page
- Review of the Principles for the Sound Management of Operational Risk, Basel Committee on Banking Supervision, October 6, 2014. Access at: http://www.bis.org/publ/bcbs292.pdf
- Riahi-Belkaoui, A. and Picur, R.D. (2000). Understanding fraud in the Accounting environment. Managerial Finance (26): 11.
- Rubino, M. & Vitolla, F. (2014). Corporate governance and the information system: how a framework for IT governance supports ERM, Corporate Governance, vol. 14, no.3, pp.320 –338.
- Samociuk, Martin, Iyer, Nigel & Doody, Helenne. 2010. Short Guide Fraud Risk: Fraud Corruption Resistance and Detection. 2 nd Edition. GBR: Farnham, Surrey, Ashgate Publishing Group.
- Samson, S., Reneke, J.A, and Wiecek, M.M (2009). A review of different perspectives on uncertainty and risk and an alternative modeling paradigm. Reliability Engineering and System Safety. Vol. 94, pp. 558– 567

- Santomero, A. (1997). Commercial Bank Risk Management: An Analysis of the Process, Journal of Financial Services Research 12:2/3 83-115 Kluwer Academic Publishers.
- Sawyer, N. (2009). Basel Committee improves market risk framework. Risk; Vol. 22, Issue 2, p. 8.
- Scandizzo, S. (2007). The operational risk manager's guide: how to understand methodologies, policies and procedures. London: Risk Books
- Schwartz R.J. & Smith C.W. Jr. (1997). Derivatives Handbook: Risk management and control. New York: Wiley
- Schwartz R.J. & Smith C.W. Jr. (1997). Derivatives Handbook: Risk management and control. New York: Wiley
- Schwerter, S. (2011). Basel III's ability to mitigate systemic risk, Journal of Financial Regulation and Compliance, vol. 19, no.4, pp.337 – 354.
- Shongotoal, I.O. (1994). Fraud Detection Prevention and Control. Lagos wwbbcnews.com/business Sulavian, A.K (2008), "Fraud Prevention and Control". Zaria, Department of Business Administration, Ahmadu Bello University.
- Silverstone, H., Sheetz, M., Pedneault, S., Rudewicz, F. (2012). Forensic accounting and fraud investigation for non- experts. New Jersey: John Wiley and Sons.
- Simister, S. (2000). Risk management: Usage and benefits of project risk analysis and management, International journal of project management, vol. 12, no.1 pp. 5-8.
- Singleton W.T & Singleton A.J. (2010). Fraud Auditing and Forensic Accounting, Fourth Edition. Published: John Wiley & Sons, Inc.
- Sinha, Anand, Deputy Governor, Reserve Bank of India speech addressed on —Perspectives on Risk and Governance, at the Risk & Governance Summit organized by the Indian School of Business, Hyderabad and Deloitte at Mumbai on August 23, 2012, electronic copy available from http://rbi.org.in/scripts/BS_SpeechesView.aspx?Id=720
- Sironi A and Resti A (2007). Risk Management and Shareholders' Value in Banking, 1st edition, Wiley.

- Sjölander, P. (2009). Are the Basel II requirements justified in the presence of structural breaks? Applied Financial Economics; Vol. 19, Issue 12, p. 985-998.
- Skousen, C.J, (2009). Detecting and Predicting Financial Stability: The Effectiveness of the Fraud Triangle and SAS N0.99, Journal of Journal of Accounting and Auditing. SSRN (Social Science Research Network), Vol. 13, h. 53-81.
- Smith, E. R. (1995). A positive approach to dealing with embezzlement. The White Paper, August/September, pp 17-18.
- Smith. N.J., Merna, T. and Jobbling P. (2006). Managing Risk in Construction Projects. 2nd edition Oxford: Blackwell Publishing.
- Smith. N.J., Merna, T. and Jobbling P. (2006). Managing Risk in Construction Projects. 2nd edition Oxford: Blackwell Publishing.
- Stoneburner, G., Goguen A., & Feringa, A. (2002). Risk Management Guide for Information Technology Systems. National Institute of Standards and Technology, NIST Special Publication.
- Storkey I. (2011). Operational Risk Management and Business Continuity Planning for Modern State Treasuries. International Monetary Fund Fiscal Affairs Department.
- Suh, B., & Han, I. (2002). Effect of trust on customer acceptance of Internet banking. Electronic Commerce Research and Applications, 247-263.
- Sutherland, E.H. (1949). White Collar Crime. New York: Dryden.
- Sutherland, Edwin Hardin (1974). Criminology (9th ed.). Philadelphia: Lippincott.
- Sutton, G., Khazanchi, D., Hampton C. & Arnold V. (2008). Risk Analysis in Extended Enterprise Environments: Identification of Critical Risk Factors in B2B E-Commerce Relationships. Journal of the Association for Information Systems, 9(3-4), p. 151- 156,158,160,164-166,168-174.
- The Dyre Wolf – Bank Transfer Scam Alert, National Fraud Intelligence Bureau and City of London Police, April 2015. Available from: http://www.fsb.org.uk/docs/defaultsource/fsb-org-uk/152/assets/april-2015/thedyre-wolf---bank-transfer-scam-alert.pd

- Thomas, P. (2009). Strategic Management. Course at Chalmers University of Technology.
- United States General Accounting Office (U.S.GAO) (1999). Information Security Risk.
- Unugbro, A. O. and Idolor, E.J. (2007). Business Social Responsibility: Concepts Strategies and Competitive Advantages, African Journal of Contemporary Issues, 7(2), pp 78-82.
- Valsamakis, A.C., Vivian,R.W.,& Du Toit, G.S. (2000). Risk Management. 2nd edition. Johannesburg: Heinemman.
- Venkat, S. (2000). Implementing a firm-wide risk management framework in the professional's handbook of financial risk management, edited by M. Lore & L. Borodovsky. Oxford: Butterworth Heinemann: 581-612.
- Venkatraman, S., & Delpachitra, I. (2008). Biometrics in banking security: A case study. Information Management and Computer Security, 16 (4), 415-430.
- Verma, M., Hussain, S.A. & Kuswah, S.S. (2012). Cyber Law: Approach To Prevent Cyber Crime. IJRREST: International Journal of Research Review in Engineering Science and Technology, 1(3), 123 – 129.
- Vinella, P. and Jin, J. (2006). Corporate governance and operational risk: a practical guide. New York: Wiley.
- Vona W. L. (2011). The Fraud Audit: Responding to the Risk of Fraud in Core Business Systems. John Wiley & Sons, Inc.
- Vona W. L. (2011). The Fraud Audit: Responding to the Risk of Fraud in Core Business Systems.Published by John Wiley & Sons Inc.
- Webb, A. (2003). The project manager's guide to handling risk. Aldershot: Gower Publishing Limited.
- Webster (1997, 1976, 1941). Webster's New Collegiate Dictionary.
- Weiss, J. W. (2009). Business ethics: A stakeholder and issues management approach. 5th ed. Cincinatti, Ohio: Cengage Learning.
- Wellink, N. (2008). A robust framework for risk management. Banker; Vol. 158, Issue 984, p. 10.

- Wells, J.T. (2005). Principles of fraud examination. London: John Wiley and Sons.
- Wells, J.T. (2005). Principles of fraud examination. London: John Wiley and Sons.
- Wiley, J. (2013). Operational Risk Management. John Wiley and Sons.
- Wilhelm, W. K. (2004). The fraud management lifecycle theory: A holistic approach to fraud management. Journal of Economic Crime Management, 2 (2).
- Willson, R. (2006). Understanding the offender/environment dynamics for computer crimes. Information Technology and people Vol, 19, No.2, pp170-186.
- Wilson D. (2000). Operational risk in the professional's handbook of financial risk management, edited by M. Lore & L. Borodovsky. Oxford: Butterwort Heinemann: 377-412.
- Wilson D. (2000). Operational risk in the professional's handbook of financial risk management, edited by M.Lore & L. Borodovsky. Oxford: Butterwort Heinemann: 377-412.
- Winch, G., (2002). Managing construction projects, an information processing approach. Oxford: Blackwell Publishing.
- Winch, G. (2002). Managing construction projects, an information processing approach. Oxford: Blackwell Publishing.
- Winch, G. (2002). Managing construction projects, an information processing approach. Oxford: Blackwell Publishing.
- Wolfe, D. T. & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. The CPA Journal, December, pp.1-5.
- Wolfe, D.T., and Hermanson, D.R. (2004). The Fraud Diamond: Considering the Four Elements of Fraud. CPA Journal 74(12) (Dec): 38-42.
- Wood, D. (2007). Basel II backlash. Risk; Vol. 20, Issue 12, p. 72-74.
- World Economic Forum (2017). Advancing cyber resilience – Principles and tools for boards, in collaboration with the Boston Consulting Group and Hewlett Packard Enterprise.

- Yogieta, S., M. (2011). Operational risk management in Indian banks: impact of ownership and size on range of practices for implementation of advanced measurement approach.
- Young R.M. (2014). Financial Fraud Prevention and Detection: Governance and Effective Practices. Published by John Wiley & Sons Inc.
- Young R.M. (2014). Financial Fraud Prevention and Detection: Governance and Effective Practices. Published by John Wiley & Sons in External Fraud Management.