NOVA IMS Information Management School

MEGI

Mestrado em Estatística e Gestão de Informação

Master Program in Statistics and Information Management

ACCESSING THE EFFECTIVENESS OF OPERATIONAL RISK MANAGEMENT AMONGTS PORTUGUESE BANKS

AYO KEHINDE OLUWAFEMI

Dissertation presented as the partial requirement for obtaining a Master's degree in Statistics and Information Management

NOVA Information Management School
Instituto Superior de Estatística e Gestão de Informação
Universidade Nova de Lisboa

NOVA Information Management School
Instituto Superior de Estatística e Gestão de Informação
Universidade Nova de Lisboa

ACCESSING THE EFFECTIVENESS OF OPERATIONAL RISK MANAGEMENT AMONGTS PORTUGUESE BANKS

Ayo Kehinde Oluwafemi

Dissertation presented as the partial requirement for obtaining a Master's degree in Statistics and Information Management, specialization in Risk Analysis and Management

Advisor: Rui Alexandre Henriques Gonçalves

November 2019

ABSTRACT

This research work was carried out to Access the Effectiveness of Operational Risk Management amongst Portuguese banks, using one of the big banks in Portugal as a case study. Operational Risk has been in existence longer than we know but the concept of Operational risk was not well defined until 1995. Operational risk exposes Organizations to diverse risks that can be quite fatal and as such gives rise to the interest in accessing how Portuguese banks manage Operational risk. The major objectives of this study was to determine whether Operational risks are effectively managed by banks in Portugal. With specific objectives such as: To access the awareness of bank employees on principles and techniques related to Operational risk management adopted by banks, to discover if banks are applying the methodologies/ techniques that allow them to mitigate operational risk correctly and to ascertain if Operational risk management improves bank results in Portugal.

Questioners and interviews were used as means of data collection in this research work backed up by theoretical and empirical findings. At the end of the research work, recommendations were made.

Keywords

- Risk: Risk can be defined as the chance of obtaining a loss as result of known or unforeseen circumstances. Also, Dominic (1993) defines risk as the volatility of potential outcomes and the outcomes could be both negative and positive. Hamberg (2000) defined risk as uncertainty about the future. As a result of passage of time a risky situation at the moment may be subject to change in the future. (Cornia, Dressel & Pfeil, 2014).
- Risk Management: Risk management is the process of identifying, anticipating and acting to mitigate risk to be within the risk appetite of an organization. Risk management ensures that organizational objectives set by the both top management and the board of directors are effectively measured, controlled and reviewed before they are implemented.
- Operational Risk Management: Basel committee on banking supervision (2001) defined Operational risk as the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and system or firm external events. The Basel 2 directive for banking and Solvency 2 for insurance has been established to focus on operational risk. (Chavez-Demoulin, 2006).
- People Risk: People risk cuts across various compartments such as mistakes, accidents, manipulation of markets, legal action, tax avoidance, mis-selling products, improper organization of work by employees that can lead to loss in an organization.
- Process Risk: Process risk a subcategory of Operational risk which involves inefficiency and ineffectiveness when carrying out business operations and activities which can lead to loss.

An example of such errors can be miscalculations, omissions, addition of wrong values. That is why it is of utmost importance for financial organizations to have active control teams to check and balance on transactional activities.

- System Risk: Information technology has both good and bad sides. Amongst the various downsides is hacking, computer viruses, phishing, etc. which accumulates to loses. System risk however is dependent on people and processes. Unlike other forms of risk, system risk is not independent. (Fheili,2011). It is advisable for companies to outsource and internally regulate systems and investment in IT.
- External Risks: external Risks are caused by external events such as Economic factors, Political and Legal factors, Natural factors such as Disasters which are beyond the reach of the company.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

INTRODUCTION

1.1 BACKGROUND OF STUDY.

Corporate organizations are constantly involved with risk and risk management when performing their daily activities, as a result the end objective of organizations is to be able to foresee and highlight risks at various levels and taking appropriate steps to be more equipped for unseen circumstances in the future. Active risk management should be a fundamental department of corporate organizations. (Jorion, 2001, p.4).

Events such as the financial crisis of 2007 which sprung up in the U.S and gradually migrated to Europe raised major awareness to risk management. Many writers and experts have stated that the issue was due to bad credit attitude, credit defaults hereby making it fundamentally a credit risk-oriented issue. However, this is true, but it doesn't show the full picture. Every form of risk be it credit, liquidity, market has its roots in operations. The Basel II accord describes operational risk as actions r activities that result in diminishing profit either by people, processes, procedures, technology both within and outside an organization.

A fundamental issue was the oversaturation of loans and mortgages at even lower rates. This encouraged borrowing and the masses were drawn to it. When it was time to repay, the default rate was really high hereby causing the financial crisis. This is a fundamental Operational risk issue because standard procedures must be put in place before new initiatives are followed. Procedures, scenarios have to be tested to know the level of risk, the risk quotient to determine if it is within the risk appetite of the organization and to know if it is really worth taking. Different perspectives have been addressed among experts as to the root cause of the crisis. (Andersen, Maberg & Hägerwzx, 2012).The bankruptcy of Barings in the early 90's triggered by a scoundrel trader robbing the bank of over a million dollars, was probably when Operational risk was discovered.

Exposing other forms of risk other than the traditional credit, market and liquidity risk. (Cruz, 2002).

Similar discussions have been raised differentiating risk from uncertainty or unpredictability.

Solvency II (Directive 2009/138/EC), elucidates operational risk as the risk of loss arising from inadequate or failed internal processes, system or personnel or from external events excluding risks arising as a result of strategic decisions and reputational risk.

Each entity is unique in the way it manages and combines technology, human resources, processes, therefore addressing Operational risk is very complex. Operational risk can take the various forms such as; errors in recording a client's data in a business transaction, incorrect figures and several others. Several arguments have been made stating that technological risk is part of operational risk while others think it's a separate entity.

Recent developments in risk management by solvency II adopted a risk-based approach which encourages competence in risk management from banks and insurance companies and also promotes proper economic assessment. For example, the solvency capital requirement for both banks and re-insurance companies requires them to maintain high level of equity to enable them cope should incase significant losses arise.

Operational risk as the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and system or firm external events. Such events can lead to financial loss through errors, fraud, fire or other disasters (Basel 1998). Prior to this, there was no generally acceptable definition of Operational risk, it was the risk that is not Credit or Market risk although the nature of banks require them to assume some financial risks, new approaches must be discovered and implemented to cope with the new financial products and services brought in by rapidly changing technology, the availability of real-time information and increased competition Timothy, G. H. (1997).

Financial institutions, banks in particular can be exposed to so many failed processes, one of major causes of failures in banks and insurance institutions can be linked to the attitude towards risk management and specifically the management of Operational risk management Hess (2001), this issue is really relevant and vital, if left unchecked can raise concerns on risk culture, risk governance etc. ((Schwarts-Garliste, 2013).

Operational risk management has sprung growing interest and there are several reasons for this move. Amongst others, one of the main reasons for this move is the reporting of Operational losses by various financial institutions. (Acharyya, 2010). International authorities have implemented regulations to mitigate operational risk. For example, the Sarbens Oxley Act (SOX). This directive is mandatory for all institutions listed in the United States stock exchange with the purpose of restoring public confidence in Financial reporting, auditing and Financial markets. (Forcht &Luthy 2006). The same applies in Europe. The (EUROSOX). Also the Basel Accord which is compulsory for all financial institutions within the European union (Moosa 2007). There are several approaches to calculating the capital required to account for operational risk. Banks take several approaches towards operational risk namely: Risk acceptance, Risk refusal, Risk mitigation, Risk reduction and transference. Because of the synergy between operational risk management and capital requirements, banks would rather mitigate, transfer or totally eradicate operational risk (Flores et al 2006). Banks are regulated by the Basel accord while insurance companies are guarded by the solvency II directive however, they are somewhat similar.

This study examines how banks manage operational risk in their day to day activities. banks should ensure that before products, activities, processes and systems are structured, they are subject to strict Operational Risk Management assessment procedures. However, time series of records could be used to track the severity of loss and this can be useful in assessing the Organization's exposure to operational risk and developing a policy to mitigate that risk.

1.2 STATEMENT OF RESEARCH PROBLEM

Operational Risk management is important because risks is present in every organization. Operational Risk can be said to be the oldest Risk facing Financial institutions, but most top management argue that Credit Risk has more impact on a company. Deregulation and globalization of financial service together with growing sophistication of financial technology are making the activities of financial institutions (and their risk profiles) more diverse and complex (Dowd, 1998) Developing practices suggest that Risks and other Credit, Insurance and Market Risk can be substantial. (Basel,2001). Examples of Risks that are faced by banks are the use of automated technology and thus has the potential to transform manual to system failure risk. Because of highly automated technology, greater relevance is placed on globally integrated systems. Banks have almost universally embraced on upgrading their operation Risk Management and control systems (Santomero, 1997). This study will access the effectiveness of Operational Risk management in Portuguese financial system, using a case study of one of the biggest banks in Portugal.

1.3 OBJECTIVES OF STUDY

Based on the work of Rui Gonçalves, the researcher has formulated a main objective and three specific objectives. They include:

Main objective:

To determine whether Operational risks are effectively managed by banks in PortugalThe specific objectives include:

To access the awareness of bank employees on principles and techniques related to Operational risk management adopted by banks.

Also, to discover if banks are applying the methodologies/ techniques that allow them to mitigate operational risk correctly.

Furthermore, to ascertain if Operational risk management improves bank results in Portugal.

1.4 SIGNIFICANCE OF THE RESEARCH

Large losses are infrequent as such most banks don't have adequate historical and time series data on causes and adverse effects of Operational risk. Although many argue operational risk is relatively new compared to Credit and market risk, studies revealed that banks have progressed in managing Credit and Market risk compared to Operational risk. Operational risk stems from more complex sources compared to other risk types. For example, banks with simiFlar portfolios in terms of assets and liabilities will most likely have the same credit and market risk but they tend to differ significantly in terms of Operational risk (Holmes 2003). In view of the foregoing, this study provides practical guidance on how banks can effectively manage Operational Risk. Bank managers would benefit from this research by adequately utilizing the findings and applying them in restructuring their Operational Risk Management Programs. This research distinguishes between the direct and indirect impacts of the causes of operational risk as it could be human, technological factors. Also, it is possible to identify the causes of operational risk such as unexpected loss as a result of internal errors, poor supervision, and so on.

Furthermore, this study will contribute to build knowledge on methods used to manage Operational Risk and provide further suggestions to the improvement of Operational control practices and Risk monitoring in Financial Institutions.

LITERATURE REVIEW

2.1 BACKGROUND

Operational risks can be linked to be one of the root causes of many financial failures over the past decade. Factors such as little or inadequate knowledge of risk sources has resulted in inadequate risk Management. (Sinha, 2012). Improvements such as strengthening the risk culture, raising awareness of risk and risk exposures would go a long way in improving risk management. Risk exposures can be measured both quantitatively and qualitatively to accurately capture the magnitude of risk and its impacts. Quantitatively, risk exposures can be measured numerically while qualitatively risk exposures can be measured subjectively in terms of high, low and average impacts (Sinha,2012). Studies showed that the concept of Operational Risks is not new as they comprise of Human mistakes, fraud, theft, process failure, system errors and external hazards such as fires and floods.

Previously, the impact of operational risks was relatively insignificant though its application varied by institutions, Basel III for banks and Solvency II for insurance companies, the idea stays the same. Trends have made operational risk more significant than ever before. With increasing requirements, complexity and volume of risks, information systems are believed to provide benefits for risk management activities.

Studies ascertain that majority of international banks already commenced accounting for operational risk by allocating reserves to cater for operational risks over other risks. The granularity and importance of operational risk is dependent on the industry and market where the organization is present. Operational Risk differ from other forms of Risks (credit and Market Risk) as it doesn’t yield any return. Operational risk is present in every organization as a result, without the proper management of operational risk, significant losses may arise.

Information systems is of great advantages considering the complexity of risks. Information management helps to integrate operational risk activities while also optimizing operational risk management performances. Operational risk management can be improved by adequate information management. According to (Lam and Arnold, et al), performance management systems support Risk Management process.

2.2 BANKS AND RISKS

There are many definitions of risk. Risk can be defined as the probability of the occurrence of an adverse/negative event or incident that might leave a negative impact on the organization (yang 2011). Any decision is a risk and risks can be measured by several factors like occurrence, severity and so on. (Mazouni,2008) emphasizes that the key factors severity and the frequency of the occurrence of an event. From the above we can deduce that risks have probabilities of occurrence and there is an extent to the severity of impact of risks.

Risks are uncertain conditions that if they occur, could affect the ability of an organization to achieve its goals. (Tuncel, Alpan 2010) also, (Baker teal.,2012) defines risk as an uncertainty that can be expressed in terms of probabilities.

Risk can be defined as the chance of obtaining a loss as result of known or unforeseen circumstances. Also, Dominic (1993) defines risk as the volatility of potential outcomes and the outcomes could be both negative and positive. Hamberg (2000) defined risk as uncertainty about the future. As a result of passage of time a risky situation at the moment may be subject to change in the future. (Cornia, Dressel & Pfeil, 2014).Banks are in the business of taking and managing risks (Arora,2009). Banks act as intermediaries in transforming risk resulting to risk warehousing (Sinha,2012). Over the years, the activities of banks have become more complex and sophisticated as a result of risk. The behavior of banks towards risk taking and aversion has a huge impact on financially and economically. Banks thrive on public confidence and as such any breach in confidence can lead so severe losses and eventual liquidation of banks (Sinha,2012). For this reason, a sound risk management system is vital for banks to thrive.

2.2.1 TYPES OF RISK

Risks are of various types and forms. Some are Insurable while others are un-insurable. The concept of insurability and in-insurability is determined to a large extent by a company's risk retention profile/policy. The classification of risks is based on cause and effect (Dionne,2013).

Banks face various risks which can be divided into two broad categories namely; business and control risk. Business risks stem up from the day to day operations of the bank and consist of eight types of risk namely; credit, market, capital, liquidity, operational, business strategy, systemic, moral hazard. While control risks are risks that arise as a result of the inability of internal controls, management and compliance to capture lapses in operations.

The three categories of risk mentioned in the Basel capital accord are credit risk, market risk and operational risk.

- **Market risk**: it is the risk of loss due to decline in assets as a result of movements in market factors and forces. Such forces include recession, political instability, interest rate and foreign exchange changes, natural disasters and terrorist attacks etc. market risks are mostly related to investment banks because they are active in capital markets. Mckinsey defied market risk as the risk of loss as a result of changes inequity prices, interest rates, credit spreads, foreign exchange rates and other indicators whose values are set in a public market.

- **Credit risk**: it is the risk of a company's inability to pay its debt. It can be complete or partial. It is also the risk that a lender might not be able to repay his loans. Credit risk default can lead to loss of principal plus interest. To reduce credit risk, banks must increase interest rate for borrowers with high credit risk. Unsteady income, low credit score, employment type and availability of collateral determines the Credit risk associated with a borrower.
- **Operational risk**: Operational risk is a risk of loss occurring due to deficient or failed internal process, people and systems, or from eternal events. Basel committee on banking supervision (2001) defined Operational risk as the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and system or firm external events. The Basel 2 directive for banking and Solvency 2 for insurance has been established to focus on operational risk. (Chavez-Demoulin, 2006).

2.3 RISK MANAGEMENT

According to (cheng,Yip & Yueng, 2012), risk management is said to be a cycle or a road map that can be used to make detailed and informed decisions to accept a risk, eliminate the adverse effects of hazardous events or to reduce the probability of a hazardous event occurring.

Risk management involves procedures, policies, actions and tools used to manage risk and make them acceptable (Alhawari et al, 2012). The institution of risk management (IRM) defines risk management as a helpful process through which organizations understand, evaluate and take actions on all its risks with a view of increasing the probability of success and reducing the probability of failures.

It also involves managing risk by developing diverse management strategies to avoid risks, minimize the negative effects of taking up the risks and accepting some or all of the consequences that comes with each risk.

2.3.1 RISK MANAGEMENT CONCEPT AND PRINCIPLES

Organizations encounter risks while trying to achieve the objective, and as such they began to search for approaches to effectively manage these risks. The concept of risk management has grown over the last decade thereby becoming one of the most important management skills.

At early stages, organizations focused on building strong financial approaches to withstand the negative impacts of uncertain events but now, organizations have taken a broader look towards risk management by acknowledging that risk management applies to both negative events and positive opportunities that they must take advantage of. Therefore, a proactive approach must be followed to find out possible threats, impacts of the threats and positive outcomes of taking up risks in deciding whether to take up or avoid them.

Organizations exist to make profit, which cannot be attained without taking risks and the risk must be effectively controlled. To make profit, an organization must take advantage of opportunities, focus on upside risk while simultaneously reducing the volatility of earning indicators.

Previous reviews show that risks were managed in silos, for example, the main focus of risk management approach in the banking sector was on credit risk, market risk, operational risk and credit risk while for insurance sector the focus was on risk of underwriting and investment functions. Many of the global reinsurers like Swiss re, have invented a new technique to manage risk called Alternative risk transfer (ART) used to manage risk with high severity but low frequency (Culp, 2012)

The introduction of solvency II directive by the European union helps insurance companies to manage their risks effectively and enforce organizations to pay more attention to managing all the risks they are exposed to. Solvency II comprises of three pillars; pillar one emphasizes on qualitative requirements, pillar two focuses on the requirements of corporate governance while pillar three emphasizes on disclosure and transparency. This directive gives insurance companies the opportunity to improve risk management skills and efficiency of internal operations.

2.3.2 RISK MANAGEMENT TOOLS

Different risks have diverse characteristics. Based on these diverse characteristics, the tools for managing the risk is determined. There are many tools used in risk management. In selecting tools for managing risk, many factors must be considered lie cost, effectiveness and efficiency. (Dofrman, 2012).

Example of such tools include:

- **Loss prevention**: loss prevention involves the reduction of the liabilities of an event while also reducing the magnitude of an event that dies occur.
- **Damage limitation**: damage limitation is concerned with reducing the magnitude of events that occur.
- **Risk treatment**: this tool involves all activities to control and reduce the magnitude of risk. Also constructing risk to an acceptable level
- **Risk financing**: risk financing involves determining when to pay for losses and who pays it

- **Risk tolerance**: the exposure may be tolerable thereby needing no further action being taken even if it is not tolerable, the ability to do anything about some risks might be limited.
- **Risk transfer**: the best option for some risk is to transfer them either by re-insurance or by third party. This option is best for reducing financial risk.
- **Risk termination**: some risk may only be treatable or contained to acceptance level by terminating the. Especially when the risks are way above the company´s quota.

2.4 OPERATIONAL RISK

It wasn't up until the late 90's when the Basel committee introduced Basel II hat operational risk got maximum recognition. The committee identified risk s from human misbehaviors such as mistakes, acts of fraud, theft which at the time were not covered by other types of risk management hence Operational risk was defined by the committee as risk incurred by inadequate or failed internal processes, people, systems or external events (Basel,2006) The modification of the definition can be used by several institutions to suit their context.

Operational risk is further divided into special categories namely;

- People Risk: People risk cuts across various compartments such as mistakes, accidents, manipulation of markets, legal action, tax avoidance, mis-selling products, improper organization of work by employees that can lead to loss in an organization.

- Process Risk: Process risk a subcategory of Operational risk which involves inefficiency and ineffectiveness when carrying out business operations and activities which can lead to loss. An example of such errors can be miscalculations, omissions, addition of wrong values. That is why it is of utmost importance for financial organizations to have active control teams to check and balance on transactional activities.

- System Risk: Information technology has both good and bad sides. Amongst the various downsides is hacking, computer viruses, phishing, etc. which accumulates to loses. System risk however is dependent on people and processes. Unlike other forms of risk, system risk is not independent. (Fheili,2011). It is advisable for companies to outsource and internally regulate systems and investment in IT.

- External Risks: external Risks are caused by external events such as Economic factors, Political and Legal factors, Natural factors such as Disasters which are beyond the reach of the company.

- Internal fraud; this constitutes of losses incurred due to intentional or inappropriate acts performed by employees/ stakeholders involving breaking laws, regulations or organizational policy.
- Damage to physical assets; this involves losses because of intentional damage or natural disasters that affect the assets of the organization in a negative way.
- System failures; this involves the losses due to system failures.
- External fraud; this constitutes of losses related to inappropriate use of property, information breaches.
- Delivery process Management; losses related to Process Management, transaction processes, etc.

Operational Risk is an integral part of Enterprise Risk management as it is well known and identified by the Banking and the Insurance Organizations

2.4.1 CHARACTERISTICS AND IMPORTANCE OF OPERATIONAL RISK.

Operational Risk is birthed when employees, systems, and processes of companies are impacted by external events, in which case Operational Risk emerges before both credit and market risks. Over the past fifteen years, Operational Risk has been estimated to be one of the major sources of Financial losses to the Banking and Insurance sector. Al Berman (2015) stipulated that it is more profitable for banks to accept certain levels of risks while also pursuing risk avoidance. Although, it is the consequences of a loss event that determines the occurrence of an Operational loss event. A study reported by KPMG (2006) grouped the importance of risk management into three sections. The first being to prevent risk by educating employees on operational risks and its effects within the frame of the organization. The second section is channeled towards reducing the impacts of risks that already occurred to ensure business continuity and the third being to have measures in place to target risks caused by potential threats.

Therefore, Operational risks can materialize directly or indirectly through Market or Credit Risks.

Operational Risk versus Market and Credit Risk:

- Operational Risk does not have a direct relationship with risk and return as higher operational risk do not lead to better or higher income.
- Financial institutions lack event data/ time series data of operational risk as opposed to Credit and Market Risk as loss events as loss events in an institution are not necessarily transferrable to other institution
- Unlike Credit and Market Risk where it is easy to measure, control and differentiate risk factors and risk potentials, establishing links between risk factors and the probability or severity of losses in Operational risk is more difficult.

- It is relatively infrequent for Operational losses to threaten the stability of a credit institution.

2.4.2 PRINCIPLES FOR THE SOUND MANAGEMENT OF OPERATIONAL RISK

The assignment of roles and responsibilities is of utmost importance and a very crucial aspect in formulating Operational risk frameworks, and as such should be coordinated carefully for adjustments. The basel committee on bank supervision (2003) articulates expectations in relation to bank governance activities and the requirement of bank's risk management framework.

The following principles are used by banks when developing and updating their risk framework and as checklist when regulators are assessing the operational risk management and capital adequacy of individual banks.

- The board of directors of the bank must ensure that there is an appropriate risk culture, an appropriate risk management framework and a clear statement of the bank's risk appetite and tolerance.
- The Top Management has the responsibility of designing and implementing the Risk strategy and as such they ought to be involved in the stages of decision making. Top management should provide adequate funds and Human resources to execute Operational Risk Management. Top management is expected to put in place policies and procedures for managing Operational risk management for all bank products, activities, processes and systems that are consistent with the board's risk appetite and tolerance.
- Risk Identification: Means of identifying operational risks must be in place for all bank activities, products, systems.

- Control and mitigation: there must be robust controls and risk mitigation and risk transfer strategies put in place for example business continuity plans must be in place should incase unpredictable and unforeseen contingencies arise.
- Monitoring and Reporting: Processes to monitor report operational risks profiles and material exposures are required.
- Disclosure: Banks are required to disclose how they manage Operational risk as well as details of risk exposures and capital requirements in their annual reports.

2.4.3 OPERATIONAL RISK LIFECYCLE.

Risk Management is very vital in every organization as it helps top management identify and integrate various plans and decisions to prevent Operational risk chaos. According to (Mazouni, 2008; Tuncel and Alpan 2010), risk management can be categorized into four cycles namely:

- Identification and Assessment of Risk
- Treatment of Risk
- Controlling Risk
- Monitoring and Reporting Risk

Risk Identification: Financial institutions must be aware of potential risks to control and limit them. Each credit institution has internal control systems and guidelines in identifying and limiting potential risks. Through the process of identification risk sources and risk drivers a financial institution takes preventive measures in dealing with risks. PWC (2013) points out that risk identification s vital for accurate operational risk monitoring and control to take place. During the process of risk identification, financial institutions consider factors such as:

- Type of customer

- Risk culture and tolerance of the company
- Design, implementation and effectiveness of process and system.

Using the following tools:

- Risk indicators
- Loss databases
- Risk inventory
- Scenario analysis.

Coupled with external data a loss database is useful in qualifying and modeling operational risk.

Risk assessment: Also known as risk inventory, it is aimed at identifying operational risk and making decisions to either take up or avoid the risks. Every organization faces diverse form of risks and they must be effectively accessed (Andrew,1995). The main purpose of risk assessment is to identify significant operational risks and eventually evaluating the risks. They usually take the form of questionnaires, workshops and interviews. Qualitative evaluations obtained help to determine the severity of loss and help in ranking risks to identify major risks. The risk portfolio can be presented as a risk map or matrix which presents strengths, weaknesses, opportunities and threats of the organization. Risk assessment may have different orientations such as:

- Risk orientation
- Control orientation
- Process orientation
- Goal orientation.

Risk Treatment: Operational risk can be treated in many ways/such as:

- Risk Avoidance: it is the strategic avoidance/elimination of hazardous activities that affects an organization´s assets. Risk avoidance seeks to avoid compromising/hazardous events in its entirety.

  That is why banks do not accept or take up every risk. Banks should avoid risks if its risk margin for activities is lower than the expected risk cost of taking all the risk.
- Risk Mitigation: Risk mitigation is the process by which an organization introduces measures to minimize or eliminate unacceptable risks. Banks develop mitigation strategies to intellectually reduce the severity of impact/probability of occurrence of such unacceptable risks
- Risk sharing and Transfer: Risk sharing, and transfer occurs if risk cannot be totally borne by a bank/ insurance company, In the sense that the risk cannot be adequately reduced, or the cost of control is higher than the cost of expected loss. Also, a risk should be shared or transferred if the risk is too high in relation to the company's risk appetite. An example of
- risk sharing is outsourcing of activities and functions. There are cases where risks can be shared and not fully transferred.

Risk Control: involves strategies and methods through which organizations identify and evaluate potential losses while taking adequate precautions to reduce or totally eradicate such potential threats. Organizations should put in place control measures in their business processes performed by employees (Andrew,1995). Also, separate inspections by internal and external entities, supervisory board, auditors, auditors and certified public accountants acts as safeguards against the acceptance of inappropriate risks that is out of the organization´s risk profile. And as such all parties involved must corporate to avoid control gaps.

Companies can carry out continuous monitoring which is the process of detecting risks and compliance related issues associated with an organization ´s financial and operational environment. In this process, only employees should monitor the process quality and there shouldn´t be any delegation of responsibilities to internal and external auditors. Schemes should also be put in place to motivate employees as well as sanctions in case of failures. They can also carry out separate inspections which can be carried out by internal/external auditors as well as supervisors. There should be regular follow ups to ensure that short comings are eliminated, and adequate recommendations are put in place.

Risk reporting and monitoring: Control measures identified by organizations to mitigate risks should be implemented and the effectiveness of such measures should be monitored appropriately. Risk management procedures must be flexible to ensure that new risks are assessed and addressed as soon as possible. There should be periodic checks put in place because risk management isn't a one-time procedure but an ongoing process.

2.5 DATA COLLECTION FOR OPERATIONAL RISK MANAGEMENT

Prior to Basel II there was no capital requirement for operational risk management because Operational risk was still at infancy stage. Under the Basel II accord, senior management is to put in place policies and procedures for managing Operational risk management for all bank products, activities, processes and systems that are consistent with the board's risk appetite and tolerance. In order for top management to do this, data must be present to valuate operation risk.

2.5.1 TYPES OF LOSS DATA

- Internal loss data
- External loss data

Internal loss data involves information about losses or loss events that are incurred by banks internally.

External loss data involves information about losses or loss events that are external to the bank or losses incurred at other banks.

Internal data gives useful information regarding cost incurred through risky events. internal data helps a bank determine the actions to be taken towards reducing the risk of losses. This type data is the most effective. however, it is somewhat difficult to collect good quality data. As a result, banks gather loss information experienced and other banks. Data bases such as ORX allows banks to share loss data for operational risk.

There are several issues that accompany collecting loss data such as:

- Employees may be unwilling to identify internal failures and reporting risk events.
- Loss events of high value do not necessarily mean all loss events are captured also, loss events with low value might make it difficult to record loss events as it may be difficult to quantify.
- events that almost led to losses should also be recorded: Because there are no losses now do not mean that those events are risk free.
- Collecting and compiling loss data for banks with branches in different locations is difficult especially when standards vary.

2.6 **CAPITAL CALCULATION FOR OPERATIONAL RISK IN BASEL III**

The basel III framework is an improvement from its predecessor basel II in the sense that it addresses shortcomings in the pre-crisis regulatory framework by providing a resilient foundation for the banking system. (BCBS, 2017).

The basel III reform introduces the standardized approach to replace the already existing approaches to calculate minimum capital requirements for operational risk. Under the standardized approach, minimum capital requirement for calculating operational risk capital is :

Operational risk capital = Business indicator component * internal loss multiplier. The business indicator component is calculated by multiplying the business indicator (BI)*(α). Both components have a positive relationship as an increase in (BI) also leads to an increase in (α). For example banks with business indicator (BI) of (less than or equal to) one billion, they have an alpha (α) of 12%, and they belong to the first basket banks with business indicator (BI) of (more than)one billion but (lower) than thirty billion , they have an alpha (α) of 15%, and they belong to the second basket. banks with business indicator (BI) of (greater than) one billion, they have an alpha (α) of 18% .(BCBS,2017).

The internal loss multiplier is calculated by: Lm= (exp(1)-1+$(lc/bc)^{0.8}$). Loss component (LC)= 15* amount of losses incurred from operational risk over the past ten years. At any point in time where the business indicator and the loss component is equal, the loss multiplier is equal to one A bank is required to hold higher capital if the (lc) is greater than the (bc)and vice versa due to the incorporation of internal loss to the calculation methodology.

BCBS (2017) stated that banks who currently do not possess up to ten years of high quality loss data should use five years of high quality data, and those who have no quality loss data should make use of only the business indicator component (BI) for smooth and easy transitioning into the standardized approach which is to commence in January 2022.

METHODOLOGY

3.1 RESEARCH METHODOLOGY

In this chapter, methods and measures adopted in conducting and gathering data for this study. It includes the report of the population of study, sampling techniques, sample size, sources of data, method of data collection and method of data analysis and testing hypothesis.

It is to be observed that the research procedures implemented for any study is to a large extent controlled by the nature and objectives of the study. A qualitative approach has been followed in this research. Data was collected from two sources: primary and secondary sources related to the study topic. The secondary sources used during the literature review were retrieved from books, journals articles online, research and annual reports. The primary sources were gained through interviews designed by the researcher.

The purpose of this research is to access the effectiveness of operational risk management amongst the Portuguese financial system.

3.2 RESEARCH APPROACH

The procedures utilized in this study were based on a series of research questions designed to identify and access the effectiveness of operational risk management amongst the Portuguese financial system.

For the purpose of this research, the researcher has conducted the study that utilizes exploratory research to shed light accessing the effectiveness of Operational risk management amongst the Portuguese financial system and make recommendations.

Exploratory research according to Robson is a valuable means of finding out what is happening in order to seek further knowledge, to ask questions and to access phenomena in new light, (Saunders, Thornhill, 2009). This type of research is used when the researcher notices new insight or ideas and wants to figure it out. There are two types of exploratory research: “new angle” and “new topic”. “New topic” research refers to the study of a brand-new idea and usually it produces results while “new angle” research changes the perspective of understanding a particular topic either by discovering a new method or by viewing the topic from a new theoretical perspective. (Finn, white, Walton, 2000). This study was conducted with operational risk executives of a selected bank in Portugal. The interviews were designed to generate a written response so that the interviewees could provide answers in their own words and also for accountability.

3.3 RESEARCH DESIGN

Research design is the plan and structure used for the study in order to obtain applicable answer to research questions (Creswell & Clark 2011).

The study starts with setting the research objectives, and then the researcher utilized the literature review to have an in-depth understanding of the study topic. The thirst step involves conducting interviews with experts in the Portuguese financial system to understand the current state of operational risk and operational risk management situation. A mixture of both the qualitative enquiry approach and a qualitative approach was used to explore operational risk amongst the Portuguese banks. A minimum of seventeen operational risk masters were selected for an interview of which thirteen people participated, also thirty non-operational risk masters cutting across the I.T and several other departments participated by answering the questionnaires. According to Denzel (2005), a minimum of ten interview respondents or participants are enough render a research finding valid. The names of the respondents and the company they work for are kept secret for confidential reasons.

Finally, based on the results, a risk management framework will be developed for the Portuguese financial system.

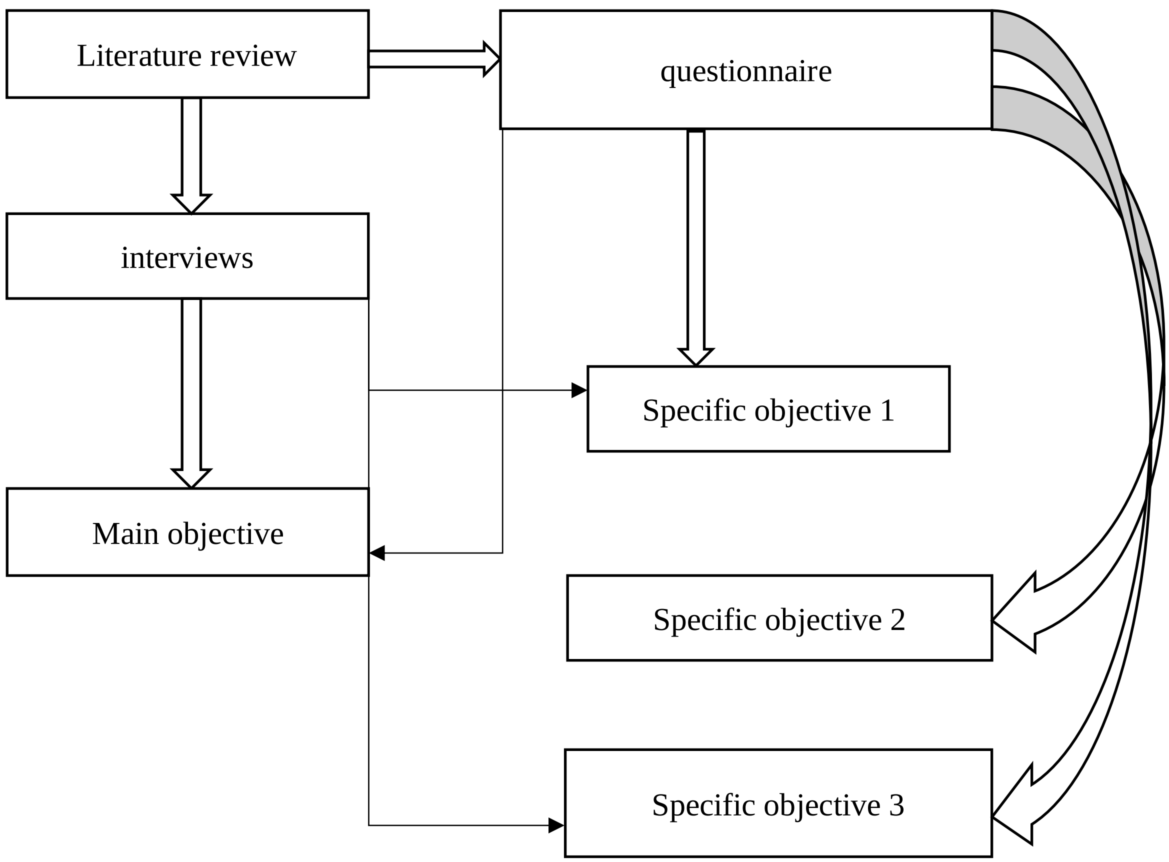

Figure 1: Research Design. (Source: Ayo Kehinde "accessing the effectiveness of operational risk management amongst Portuguese banks 2019)

3.4 DATA COLLECTION

The data used for this study is derived from the primary source. The researcher through the use of interviews, carefully crafted questionnaires and direct observation collected primary sourced data. An interview consists of series of questions for the purpose of gathering information from respondents. An interview provides insight on organizational issues and activities through the use Thus, these questions are derived from the research statement, research question, and research objectives. Interviews can be used to gain insight on organizational issues by understanding the perspective and living in the personal experience of who lived it (Denzil,Lincoln,2005). This means of data collection provides answers to most complex and sensitive questions.

The interviews were open-ended and were constructed via mail after meeting the respondents and explaining what the aim of the interview is. Open ended interviews are less controlled and give an accurate description of an individual's experience and perception.

The first stage was communicating with operational risk management experts at a selected bank requesting their consent on participating in this interview session . once they agreed, a face to face session was in place to explain the questions to them after which their response were delivered.

Questionnaires were also used to collect and record initial information about the research topic, and they can be defined as a tool containing a set of questions designed for the purpose of getting specific information from the respondents about the research area.

The questionnaire included a series of close-ended questions to measure the effectiveness the operational risk management amongst the Portuguese financial insurance companies. The answers to each question asked in the questionnaire ranges from one to five following the Likert scale.

One represents strongly disagree, two represents disagree, three represents indifferent, four represents agree and five represents strongly agree. A sample size of forty non-operational risk respondents were selected to get a different view and also to account for the validity of the responses obtained from the operational risk masters of which only twenty-seven respondents participated.

3.5 DATA ANALYSIS

For the case of this study, data was analyzed using the concept of content analysis. Content analysis is a research tool used to systematically summarize qualitative data in a quantitative way, with the objective of transforming large amount of text into a highly organized and concise summary of key results. It can be used to analyze in various formats such as texts, interview transcripts , speech in both digital and printed form. Content analysis can be used to decode the message being passed across and the tone or form in which it is being passed across. (Schreier 2012).

RESULTS AND ANALISYS

In this chapter, I shall be testing analyzing and interpreting the data obtained from respondents through the use of content analysis. the data received from the findings are represented in summary tables.

4.1 DATA PRESENTATION AND INTERPRETATION

The data was analyzed based on the following objectives:

Main objective:

To determine whether Operational risks are effectively managed by banks in Portugal

The specific objectives include:

To access the awareness of bank employees on principles and techniques related to Operational risk management adopted by banks.

Also, to discover if banks are applying the methodologies/ techniques that allow them to mitigate operational risk correctly.

Furthermore, to ascertain if Operational risk management improves bank results in Portugal.

Question	RESPONSES	OPERATIONAL RISK DEPARTMENTS	NON-OPERATIONAL RISK DEPARTMENTS
The main operational risks that affect your company	Human errors I.T issues Others	8 3 2	19 5 3
How does the company identify operational risks?	ECB guidelines Risk maps and auditing	5 8	9 18
how does the company manage operational risks?	Close analysis and analysis of operational risk incidents Publicizing procedures	7 8	13 16
How effective are these techniques in managing operational risks?	Very effective	13	27

	(prevent and track risk and report anomalies to prevent re-occurrence)		
What type of impact does operational risk have in your company?	financial and reputational other	12 1	23 4
What do you as the prime objective of operational risk departments?	identify and mitigate risk	13	27
Does the company maintain a clear, accurate and updated record of the operational risks they face?	Yes No	13 0	27 0
What regulatory approach under the basel accord is followed in your company in calculating and allocating capital against operational risk?	Advanced Measurement Approach (AMA).	13	
Do you think that there are positive impacts of operational management on organizational results? how?	Yes (Helps to minimize errors, improves credibility amongst others)	13	27
In your opinion, should the company have an independent operational risk management department? Why?	Yes (for better performance and independence)	13	27
Do you think operational risk management in your company covers the most severe situations that can and may appear?	Yes	13	27
Does the organization you work for provides training on operational risk management?	Yes No Not enough	13	16 11
Are company procedures updated and communicated to the employees regularly so as to reduce operational risk?	Yes No	9 4	22 5

Table 1: (Source: Ayo Kehinde "accessing the effectiveness of operational risk management amongst Portuguese banks 2019)

From the data gathered trough the interview and the questionnaire the follow can be stipulated:

1. The main operational risks affecting the bank are Human errors, I.T issues amongst others. Twenty seven respondents stated that Human errors play is the most occurring operational risk while eight respondents suggested that I.T issues play a part in operational risk of the company due to slow and crashed systems, long processes to complete task, and the remaining five respondents state that external and internal fraud accounts plays a part in the operational risk of the company.
2. The company uses the European central bank guidelines, risk mapping, auditing and procedure reviews to identify operational risk in banks. Twenty-six respondents state that risk maps are used by the bank to identify operational risk. This is done by creating potential incidents to log any Operational incident. While thirteen respondents state that the European central bank guidelines are used to identify risks that qualify for operational risk.
3. The company manages risk mainly by closely analyzing operational risk incidents as they occur and by publicizing procedures to employees to act as guidelines in their operations. Twenty respondents state that the company analyses operational risk by assigning certain teams such as the risk management team to closely watch and analyze operational risks as they occur while twenty four respondents state that the company manages Operational risk by publicizing procedures to employees to act as guidelines in their operations and to allow employees follow the new trend. Procedures can contain latest improvements and changes to the previous directive used in the bank.

4. The methods used by the company to manage operational risks are very effective as they are able to prevent and track risk and report anomalies to prevent re-occurrence.
5. Operational risk has both financial and reputational impacts on the organization. Respondents stipulated that if the company has a very high operational risk, the company image would be in jeopardy thereby affecting the financial capacity of the firm as the public perception of the company would be flawed, leading to low clients and low funds. Other respondents stated that operational risk has credit impacts as it can affect the company's credit rating.
6. The prime objective of operational risk departments is to identify and mitigate operational incidents as much as possible by performing controls and monitoring operational teams and also creating awareness of operational risk to operations teams.
7. Yes, the company maintains a clear accurate and updated record of all operational risks the company has historical data stored in the company's database that includes past operational risk events faced and this helps them in making future decisions.
8. From the results received from Operational risk managers, the regulatory approach under the basel accord is the (AMA) advanced measurement approach.
9. All respondents state that Operational risk management has positive effects on organizational results as it can contribute to minimize/ prevent operational incidents within operational teams, and this will contribute to reduce the negative impacts in the company's books as well as reduce the potential reputational damage. Also, as incidents are recorded, it prevents future impacts and the origin of the failure can be monetarized and mitigated this in turn allows the company to provide better services to its customers.

10. All respondents state that the company should have an independent Operational risk management department to centralize the information, for better and unbiased evaluation and analysis of operational risk.
11. All respondents state that the company's operational risk management covers the most severe situations that can and may appear. Also, all a lot of respondents also stated that although the operational risk management covers the most severe situations that can occur, the company can still improve on the existing framework.
12. All Operational risk managers state that the organization provides training on operational risk management and if the existing framework is applied correctly, all predictable situations and impacts should be accounted for with mitigating plans in place. All non-operational risk respondents agreed with the Operational risk managers while eleven of them also stated that although the company provides trainings on Operational risk, the trainings are not enough as they do not encompass all possible operational risk scenarios.
13. Nine of thirteen Operational risk managers stated that company procedures are updated and adequately communicated to employees regularly to reduce the likelihood of operational risk. Twenty-two of twenty-seven non-operational risk teams also followed the same initiative. while the remaining four operational risk managers and five non-operational risk teams stated totally disagreed that the company's procedures are not updated regularly as in some cases it takes more time than necessary to update policies and procedures.

SUMMARY, RECOMMENDATION AND CONCLUSION

In this chapter, a brief summary of findings, conclusions and recommendations obtained from the research work will be presented. The recommendations are to enhance the current situation of operational risk management amongst Portuguese banks. This chapter also suggest areas for further research.

5.1 CONCLUSION

This section provides findings on the link between the research main and specific objectives and the responses received via interview questions. The following was stipulated from the responses received from both interviews and questionnaires:

1) The main objective of this study is to ascertain if Operational risk is effectively managed by banks in Portugal. It was ascertained from the interaction with respondents that the main operational risks are adequately identified and managed by the company through the use of European central bank guidelines, risk maps, auditing close analysis of operational risk incidents amongst others. This conclusion is in line with the work of Andrew (1995) who stated that operational risk is assessed to identify significant risks and to evaluate the risks. Qualitative evaluations obtained help to determine the severity of loss and help in ranking risks to identify major risks. The risk portfolio can be presented as a risk map or matrix which presents strengths, weaknesses, opportunities and threats of the organization.
2) From the interaction with respondents it was coined that Bank employees are aware of the principles and techniques related to operational risk management adopted by banks. Respondents stated that although the bank provides trainings on operational risk management, it is not enough to cover all possible operational risk scenarios, majority of the respondents stated that procedures are updated and effectively communicated to

operational teams while only a few respondents stated otherwise. They also acknowledged that the main objective of operational risk management team is to identify and mitigate risks. This conclusion is in line with a study reported by KPMG in 2006 which grouped the importance of risk management into three sections. The first being to prevent risk by educating employees on operational risks and its effects within the frame of the organization. The second section is channeled towards reducing the impacts of risks that already occurred to ensure business continuity and the third being to have measures in place to target risks caused by potential threats.

3) Banks are applying techniques that enable them to manage operational risks effectively. For example : The use of the AMA (advanced measurement approach), under the basel II accord, to account for capital requirement for operational risk ,keeping accurate records of previous operational risk scenarios to prevent future re-occurrence, the need for independent operational risk departments, operational risk management accounting for the most severe situations that can occur amongst others..

4) Information extracted from the interaction with respondents showed that operational risk management improves bank results as it minimizes and prevents operational incidents within operational teams, and this will contribute to reduce the negative impacts in the company’s books as well as reduce the potential reputational damage. Also, operational risk has financial and reputational impacts on banks. The lower the operational risk, the company is exposed to more profits and more positive public recognition and vice versa. Operational risk management indeed improves bank results.

The results revealed that operational risk is effectively managed amongst Portuguese banks, bank employees are aware of principles and techniques related to risk management adopted by the banks, banks are enforcing techniques that enable them to cater for operational risk and operational risk improves bank results.

5.2 RECOMMENDATION

Based on the findings made during this research, the following recommendations are made to improve operational risk management amongst Portuguese banks. They include:

1) Companies should ensure that frequent and adequate workshops and trainings should be put in place to encompass all possible operational risk scenarios. It can be argued that the operational risks companies face increases by the day. Therefore, trainings and workshops should be frequent.
2) Company procedures must be communicated effectively. As soon as updates or modifications have been made, the company procedures must be communicated effectively adequately and with speed to reduce the company’s exposure to operational risks and losses.
3) The Basel III accord must be adopted by banks in providing adequate capital to cater for operational risks. This directive would be in full launch from the first of January 2022.

REFERENCES

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, pp.79–102

Al Berman, (2015). Risk Management and Business Continuity: Improving Business Resiliency. Risk and Insurance Management Society, Inc.

AlhawariS.,KaradshehL.,TaletA.N.,MansourE.,(2012).Knowledge- Based Risk Management framework for Information Technology project, International Journal of Information Management (32), 50– 65.

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.

Andrew, H. (1995). Banking Failures, Preventive Measures and Appropriate Responses, Causes Symptoms and Responses, the Tanzania Bankers Journal, DSM.

ArianeChapelle, Rogue trading, no training: the connections, Electronic copy available at: http://ssrn.com/abstract=2009386

Arnold, V.; Benford, T.; Canada, J.; Sutton, S.G. Leveraging integrated information systems to enhance strategic flexibility and performance: The enabling role of enterprise risk management. *Int. J. Account. Inf. Syst.* **2015**, *19*, 1–16.

Baker, A.F., El Hagla, K., Nayer, A., Rawash, A., (2012). Heuristic approach for risk assessment modeling: EPCCM application (Engineer Procure Construct Contract Management). Alexandria Engineering Journal (51), 305–323.

Basel Committee on Banking Supervision. (2001) Consultative Document Operational Risk. Bank of International Statements. [online] Available from: < https://www.bis.org/publ/bcbsca07.pdf> [Accessed: 3rd June 2018].

Basel, N. (1998). Framework for Internal Control System in Banking Organizations, Federal Reserve Bank, New York.

Basel, N. (2002). Sound Practices for the Management and Supervision of Operational Risk, Federal Reserve Bank, New York.

Basel Committee, January 2001a. Consultative Document: Operational Risk. Bank for International Settlements.

I. ——, September 2001b. Working Paper of the Regulatory Treatment of Operational Risk. Bank for International Settlements.

II. ——, January 2002a. The Quantitative Impact Study for Operational Risk: Overview of Individual Loss Data and Lessons Learned. Bank for International Settlements.

III. ——, June 2002b. Operational Risk Data Collection Exercise – 2002. Bank for International Settlements.

Basel Committee on Banking Supervision (BCBS). —International Convergence of Capital Measurement and Capital Standards||, Bank for International Settlements, 2006. Retrieved on 29th of September 2019 from www.bis.org/publ/bcbs128b.pdf

Basel Committee on Banking Supervision (BCBS). — Finalizing post-crisis reforms. 2017.Retrieved on 29th of September 2019 from www.bis.org/bcbs/publ/d424.pdf
Borrego, M., Elliot D., Amelink, C. (2009). Quantitative, Qualitative, and Mixed Research Methods in Engineering Education. Journal of Engineering Education

Castellan, C. (2010). Quantitative and Qualitative Research: A View for Clarity. International Journal of Education, Vol. 2, No. 2

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.

Chavez-Demoulin V, P. Ebrechts & J. Nešlehová (2006). Quantitative models for operational risk: extremes, dependence and aggregation. Journal of Banking & Finance, 2006, 30:10, 2635-2658.

Cheng T.C.E., Yip F.K., Yeung A.C.L., (2012). Supply risk management via guanxi in the Chinese business context: The buyer's perspective. International Journal of Production Economics (139), 3– 13

Creswell W., Clark, p. (2011). *Designing and conducting mixed method research.*

Cruz, Marcelo G., 2002. Modeling, Measuring and Hedging Operational Risk. New York: John Wiley & Sons, LTD.

Culp, C.L. The revolution in corporate risk management: A decade of innovations in process and products. *J. Appl. Corp. Financ.* **2012**, *14*, 8–26.

Dedoose. (2012) What Is Mixed Methods Research? [Online] Available from: 131 http://blog.dedoose.com/2012/10/what-is-mixed-methods-research/ 5 [Accessed: 15th May 2015].

Denzin, N.K. and Lincoln, Y.S. (2005) Introduction: The Discipline and Practice of Qualitative Research. In: Denzin, N.K. and Lincoln, Y. S., Eds., Handbook of Qualitative Research, 3rd Edition, Sage, Thousand Oaks, 1-32.

Dionne, G., (2013). Risk Management: History, Definition, and Critique. John Wiley & Sons, Inc.

Dominic, C. (1993). Facing up the Risks: How financial Institution can Survive and Prosper, John Wiley & Sons, Canada.

Dorfman, M., Cather, D. (2012), Introduction to Risk Management and Insurance, 10th edition, Prentice Hall. USA

Dowd, K. (1998). Beyond Value at Risk: The New Science of Risk, Wiley Publisher, USA.

Fabozzi, F., Jons, F., Anson, M. (2011). The Handbook of Traditional and Alternative Investment Vehicles. John Wiley & and Sons, Hoboken, New Jersey

Finger S., Dixon R. (1989). A review of research in mechanical engineering design. Part I: Descriptive, prescriptive, and computer-based models of design processes. Journal of Research in Engineering Design, Vol. 1, Issue 1, pp 51-67.

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

Finn, M., White, E., M., Walton, M. (2000*Tourism and Leisure Research Methods. Data Collection, Analysis and Interpretation* Harlow: Pearson Education.

Flores,F., Bonson-ponte, E., Escobar-Rodriguez, T (2006) "Operational risk information system: a challenge for the banking sector ", *journal of Financial regulation and compliance* ,vol. 14 No. 4, pp. 383-401.

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

Hernández Barros, R., & Martínez Torre-Enciso, M. I. (2012a). Capital assessment of operational risk for the solvency of health insurance companies. The Journal of Operational Risk, 7(2), 43-65.

Hess, K. 2011. "The impact of the financial crisis on operational risk in the financial services industry: empirical evidence", The Journal of Operational Risk, pp. 23-35.

Holmes, M. (2003). "Measuring Operational Risk: A Reality Check", Risk (16), pp. 84–87.

KPMG International. (2006). Enterprise Risk Management in the United States: A 2006 Report Card. [Online] Available from: http://www.sdabocconi.it/files/kpmg_en_version_339QIKWY11U2ZKUEHUY51224057629.pdf. [Accessed: 17th June 2019]

Jorion, P. 2001. The New Benchmark for Managing Financial Risk. New York: McGraw-Hill
Lam, J. *Enterprise Risk Management: From Incentives to Controls*; John Wiley & Sons: Hoboken, NJ, USA, 2014.

Luthy, D. and Forcht, K. (2006) Laws and regulations affecting information management and frameworks for assessing compliance, Information Management & Computer Security, 14, 2, 155-166.

Mazouni M. (2008). For Better Risk Management Approach: The Ontological Modeling Process of Accidental at Interactive System Decision Support. PhD Thesis of the National Polytechnic Institute of Lorraine, Nancy University

Patton, M., and Cochran, M (2002). A Guide to Using Qualitative Research Methodology, Medecins Sans Frotieres. PCBS. (2014) National Main Statistical Indicators. [Online] Available from: http://www.pcbs.gov.ps/site/lang__ar/881/default.aspx#Labour. [Accessed: 9th December 2018].

PricewaterhouseCoopers, (2013). Operational Risk Management, Credit Suisse Group, Zurich, Switzerland.

Moosa, I. (2007) "Operational Risk: A Survey", *Financial Markets, Institutions & Instruments*, Vol. 16, No. 4, pp. 167-200

Robson, C., (2002). Real World Research 2nd edition. Oxford, Blackwell

Sabato, S. 2010. "Financial Crisis: Where Did Risk Management Fail?", International Review of Applied Financial Issues and Economics, vol. 2, no. 2, pp.315-327.

Santomero, A. M. (1997). Commercial Bank Risk Management: An Analysis of the Process, The Wharton School of the University of Pennsylvania.

SaundersM.,LewisP.,andThornhillA.,(2009).Researchmethodsfor business students 5th edition, Perntice Hall.

Schwarts-Garliste, M.-A. 2013. "The Operational Risk Management in Banking – Evolution of Concepts and Principles, Basel II Challenges", Review of International Comparative Management, vol. 14, no. 1, pp. 165-174

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

Tewksbury, R., (2009). Qualitative versus Quantitative Methods: Understanding Why Qualitative Methods are Superior for Criminology and Criminal Justice. Journal of Theoretical and Philosophical Criminology, Vol. 1 (1).

Timothy, G. H. (1997). Risk Management, Bankers Magazine, May/June 1997, Vol 180 Issue 3 Page 10. Basel, Switzerland.

Tuncel, G., Alpan, G. (2010). Risk assessment and management for supply chain networks: A case study, Computers in Industry, Elsevier Ltd, vol. (61), pp 250–259.

Wisc. (2012) Validity and reliability. [Online] Available from: http://www.journalism.wisc.edu/~dshah/J658/Reliability%20and%20Va lidity.pdf.

Wisker, G. (2007). The Postgraduate Research Handbook, 2nd edition. Palgrave Macmillan

Yang, C. (2011). Risk management of Taiwan's maritime supply chain security, Journal of Safety Science. Elsevier Ltd, Vol. (49), pp 382– 393