Operational Risk Management Improvements within Internal Control Frameworks

Master’s Thesis 30 credits
Department of Business Studies
Uppsala University
Spring Semester of 2015
Date of Submission: 2015-05-28

Nazanin Bagherzadeh
Kateryna Jöehrs
Supervisor: Jan Lindvall
Abstract

Title: Operational Risk Management Improvements within Internal Control Frameworks
Course: 2FE840, Master’s Thesis, 30 ECTS
Authors: Nazanin Bagherzadeh and Kateryna Jöehrs
Advisor: Jan Lindvall
Date of Submission: May 28 2015

Operational Risk Management has gained attentions to itself in the recent years. Although a liquidity crisis, but Global Financial Crisis has had impacts on all areas of risk namely operational risk at financial institutions. Lessons learned by banks from the crisis forced radical changes in operational risk management structure which in turn led to many challenges. Focusing on literature and by conducting a case study on operational risk management on one of Sweden’s largest retail banks, this thesis aims on answering how operational risk management has improved by implicating risk governance and internal control frameworks. This will be achieved by getting a better understanding of critical risks threatening this bank.

The outcome of this study revealed that loss of reputation as a result of problems within IT system risks together with external card fraud are among the most common risks that banks should take into consideration when managing operational risks. It was concluded that although improvements have taken place in how operational risks are being managed, there is still room for improvements. Internal control frameworks still need to be modified by regulators to be more efficient while there should be reasonable amount of regulations applicable to banks.

Key words: Risk Management, Operational Risk, Operational Risk Management, Internal Control, Risk Governance, IT System Risk, Reputational Risk
Acknowledgement

This master thesis is the final phase at SUMA program in Accounting, Auditing and Analysis within the department of Business Studies at Uppsala University Spring 2015.

The authors would like to thank their supervisor Jan Lindvall, senior lecturer at the department of business studies, for his continues assistance and co-ordination during the writing process. Also, authors are grateful to respondents for giving access to information and the possibility to make the interviews, as well as participation in the internal seminar. Lastly, the authors are thankful to all friends and family, who helped with ideas, advices and proofreading.

Uppsala, May 28, 2015

______________________________  ________________________________
Nazanin Bagherzadeh               Kateryna Jöehrs
# Table of Contents

1. Introduction ......................................................................................................................... 1

2. Literature Review .................................................................................................................. 4
   2.1 Risk................................................................................................................................. 4
      2.1.1 Risk Management................................................................................................. 6
   2.2 Operational Risk............................................................................................................... 7
      2.2.1 Operational Risk Management (ORM)................................................................. 9
   2.3 Internal Control ............................................................................................................... 10
      2.3.1 International and National Risk Regulations and Frameworks ....................... 11
      2.3.2 Risk Reporting...................................................................................................... 13
      2.3.3 The Three Lines of Defence (3LoD)................................................................. 14
      2.3.4 Stress Test........................................................................................................... 15
   2.4 Summary of Literature.................................................................................................... 15

3. Methodology ......................................................................................................................... 17
   3.1 Research Approach ....................................................................................................... 17
   3.2 Motivation of Case Selection.......................................................................................... 17
      3.2.1 KKB - One of the four largest retail banks in Sweden.................................... 17
   3.3 Data Collection ............................................................................................................. 18
      3.3.1 Data Documentation............................................................................................ 19
      3.3.2 Respondents......................................................................................................... 19
      3.3.3 Interviews........................................................................................................... 19
      3.3.4 KKB Seminar..................................................................................................... 20
      3.3.5 Archive Searching.............................................................................................. 21
   3.4 Data Analysis ................................................................................................................. 21
   3.5 Data Quality .................................................................................................................. 22

4. Empirical Framework ......................................................................................................... 23
   4.1 KKB’s Approach towards ORM ................................................................................. 23
      4.1.1 What are the operational risks at KKB?......................................................... 24
      4.1.2 What were the ORM approaches during 2007-2014?................................. 27
      4.1.3 What are the continuous ORM approaches?................................................. 28
      4.1.4 What were the internal control procedures at KKB?.................................... 29
   4.2 Analysis ......................................................................................................................... 31
      4.2.1 Operational Risk................................................................................................. 31
      4.2.2 Operational Risk Management ....................................................................... 32
      4.2.3 Risk Governance and Internal Control......................................................... 33
5. Conclusion ..........................................................................................................................36
  5.1 Operational Risk Management and Internal Control.................................................36
  5.2 Future Research ...........................................................................................................37
  5.3 Limitations..................................................................................................................37
References.........................................................................................................................39
Appendix A.......................................................................................................................... a
Appendix B.......................................................................................................................... b
List of Figures

Figure 1. Risk Impact- Likelihood Matrix .......................................................... 5
Figure 2. Operational Risk .................................................................................. 9
Figure 3. The Three Lines of Defence ................................................................. 15
Figure 4. Summary Model ................................................................................... 16
Figure 5. KKB Risk Model ..................................................................................... 23
Figure 6. KKB Operational Risks ....................................................................... 24
Figure 7. KKB Risk Assessment Matrix .............................................................. 35

List of Abbreviations

3LoD - Three Lines of Defence
ATM - Automated Teller Machine
Basel II - The Second Basel Accord
Basel III - The Third Basel Accord
BCBS - Basel Committee on Bank Supervision
BCM - Business Continuity Management
CEO - Chief Executive Officer
COSO - The Committee of Sponsoring Organizations of the Treadway Commission
CRO - Chief Risk Officer
GFC - Global Financial Crisis
IT - Information Technologies
ICFR - Internal Control of Financial Reporting
KKB - Kungliga Kapital Banken
ORM - Operational Risk Management
PAP - Product Approval Process
SFSA - Swedish Financial Supervisory Authority
1. Introduction

“Corporations are in business of managing risk” (Jorion, 2001, p.3). Their goal is to identify risks at different business levels and take actions to be better prepared for the uncertainties in future. The goal is even stronger when it comes to financial institutions. Comparing to industrial corporations, financial institutions are more in need of active risk management (Jorion, 2001, p.4).

Traumatic and unpredictable events such as sudden changes in the economy in the last 50 years and the Global Financial Crisis (GFC) of 2007-2008 have raised more attention to risk management. Started from major U.S. financial institutions and entering Europe, there were many issues that have been neglected by risk management in different levels namely market-, credit-, liquidity-, and operational -risk. Therefore, different aspects have been discussed among experts as main reasons of the crisis (Andersen, Maberg & Hägerwzx, 2012). Strong beliefs such as “banks are too big to fail” and that they can regulate themselves, together with fuzzy risk appetite led to risk management failure in banking institutions (Sabato, 2010). Other important issues were lack of clearly defined strategy for capital allocation, disaggregated vision of risks, imperfect risk governance and ineffective internal control structure (Sabato, 2010). These were believed to be in addition to financial institutions poorly managing human factors, processes, Information Technology (IT) systems and external events related to economic situation. Therefore, the ability to avoid strong concentration and minimizing instability of returns were impaired by risk management in banks and other financial institutions.

In the last few years improvement of risk management at board level has been achieved (Munro, 2010). This was in addition to general positive changes in risk culture (ibid). But still some regulations need to be implemented. Post-crisis evidences in Europe showed that the financial reform didn’t work as expected. Banks got even bigger in size and the trade continued majorly in same way as it was before the crisis (Denning, 2013). The uncertainties are high and therefore, it is highly that in case of another crisis banks will face even more challenges to handle the crisis.

An example is the situation with the Swedish financial institutions during and after the GFC. It has been said that because of the lessons Swedes learned from the 1990’s Nordic financial
crises in Scandinavia, banks managed the recent crisis better than peer countries (Becker, Bryant & Henderson, 2012). The financial crisis decreased the profits of all major banks, but they still earned very large amount of money. Opportunistic risk-seeking behaviors together with loose control activities therefore raised the tendency of human failures such as fraud.

At present, despite the weak economic activity, main Swedish banks have good profitability and access to inexpensive funding (Sveriges Riksbank, 2014). However, it can be argued that banks, at least in Sweden, have not yet made the complete shift to better risk management approaches. At the same time the Swedish banking system has a number of vulnerabilities because of its large size and interconnection (Sveriges Riksbank, 2014). Poor internal control and risk management actions can be expected as well. Further, like banks in other countries, Swedish banking industry has made real progress toward structural changes. But banks are still working to embed policies and procedures down through each organization level as well as to embed operational risk and reputational risk in risk management processes (EY, 2013). Therefore, because of rapid changes in [operational] risk management processes Swedish banks are sensitive to various economic risks which can lead to the shock in banking system.

According to Hess (2011), one of the main causes of major failures at banks until now was the lack of attention to risk management in general and to operational risk management in particular. The relevance of this issue has grown in addition to operational risk management challenges concerning risk culture, internal control and risk governance (Schwarts-Garliste, 2013). Banks also faced new challenges with complying with internal and external regulations (ibid). Therefore, constant and comprehensive research of this issue will contribute to more coherent and effective bank operation, which in the future will help to avoid problems when major risks threaten banks.

Thus, in this thesis the focus is on Operational Risk Management (ORM) and its different components. Being quite a new phenomenon within financial institutions and banks, operational risk can be defined as “the risk of loss resulting from inadequate or failed internal processes, people, systems, or from external events” (BCBS, 2006). Since ORM deals with both internalities such as people, processes, systems, and externalities such as fraud, it is important to have enough knowledge when facing risks categorized under this group.

Based on the above, after gaining a better understanding of critical risks through collecting data, the purpose of the thesis is to identify how risk management, internal control and risk
governance have been organized to handle operational risks. The thesis will proceed by studying one of the four major Swedish banks within defined terms of ORM as the bank to major extents reflects the national economy of Sweden. This study will proceed by going through a standard risk governance model to prevent risk and manage uncertainty in financial institutions and banks, together with internal control frameworks, implemented by the bank. Considering national and international regulations, the study will give an opportunity to understand if improvements in operational risk management have occurred. Thus, after identifying the critical risks and in order to perform the purpose of this thesis the following research question must be answered:

*How operational risk management improved with implementation of risk governance and internal control frameworks at banks?*

It should be noticed here that although the recent financial crisis was mainly a liquidity crisis, it affected other areas of risk. Therefore, data collected from the time prior to, during and after the crisis will be helpful to answer the research question and to tackle the improvements.
2. Literature Review

2.1 Risk

The concept of risk is multifaceted and not always straightforward as can be seen from following studies. Referring to the ancient Greek and Italian, it becomes apparent that the word risk was used in uncertain situations and it meant “to dare” (Hamberg, 2000 & Picket, 2013, p.60). Therefore, as risk is unavoidable, humans and businesses need to dare among dynamic risk situations with unexpected outcomes (Kaplan & Garrick, 2006). It should be noted here that from early researches risk and uncertainty are not the same. According to Hamberg (2000) risk refers to situations where the probability of outcomes can be established while in uncertain situations the outcomes are unknown. Further, risk involves uncertainty, but it also might include some loss or damage (Kaplan & Garrick, 2006). In addition, what is considered risk, internal or external, in a given time might not be seen as such in future (Cornia, Dressel & Pfeil, 2014).

For a proper decision-making and to earn legitimate return on investments risks need to be weighed and measured (Kaplan & Garrick, 2006). Knowledge about the environment (Ganegoda & Evans, 2014) and the awareness of the outcomes then reduce the level of risk (Kaplan & Garrick, 2006). In business, “risks are assessed by the potential likelihood and financial impact they have, representing series of challenges that should be met and assessed” (COSO-framework cited in Picket, 2013, p.62). Assessing risks by identifying their likelihood and financial impact then helps with classifying the major risks and spare resources on the most critical ones for the business. Figure 1. presented in page 5 gives a more clear vision through this idea. The risks that are identified as high likelihood and high impact are marked as red which are the ones that threaten business more than other ones.
However, the implication of risk also depends on these two factors: 1. *Risk Culture*, 2. *Risk Appetite*.

Weaknesses in risk culture are named among main factors affecting the recent crisis (Financial Stability Board, 2014). Just like culture, risk culture is “reflected in the attitudes, behavioral, and managerial norms” within an organization which will direct the institution into the way they face and manage risk challenges (Atkinson, 2013). Moreover, risk culture has been recognized as the building block of corporate governance and ORM (Roeschmann, 2014). Yet, financial institutions (especially banks) are still facing challenges when it comes to defining a clear risk culture (EY, 2013).

Within the framework of risk culture, appropriate risk appetite is recognized and the governance makes sure that no risks are taken beyond what the culture and appetite can handle. For building a stronger risk culture throughout the organization it is important to have an effective risk appetite framework (EY, 2013). Simply defined “risk appetite is the amount of risk to which the organization is prepared to be exposed before it judges action to be necessary“ cited in Picket, 2013, p.71). The Swedish Financial Supervisory Authority (SFSA) in its latest set of regulations published in 2014 defined risk appetite as the “level and orientation of the undertaking risks that are acceptable for achieving the strategic goals of the undertaking” (FFFS 2014:1). In order to implement the right risk appetite and manage risks properly, banks and financial institutions need to link the procedure to the planning process (Finansinspektionen Regulatory Code a). It should be noticed here that risk appetite is also a dynamic factor and changes from time to time depending on the level of risks threatening the business.
Therefore, it becomes apparent that within the concept of risk, risk culture and risk appetite are also integral parts of effective bank operation and establish the basis for successful risk management.

2.1.1 Risk Management
Risk management is the main component of success in finance and investment sector today. The need for implementation of effective risk management together with corporate governance was highlighted in the GFC (Aebi, Sabato & Schmid, 2011). By adopting sophisticated risk management practices and creating the possibility of having an appropriate and sound risk management strategy; the business then will increase the likelihood of long-term survival (Kim & Vonortas, 2014). It should be noted here that the risk management process has to be fully understood by the board of directors and senior executives as well as lower-level employees.

Before, risk management has been perceived as an operational activity instead of continuous responsibility of the board (Ingley & Walt, 2008). Currently, along with board’s responsibility, risk management strategies usually focus on three main factors: meeting or exceeding an organization’s objectives, adhering to control-based objectives and complying with regulatory requirements (COSO, 2013). In addition, according to a study done by Moody (2010) to increase the effectiveness of risk management in the organization, the risk management process should be part of organizational processes and decision making while it should be dynamic and responsive to changes.

Within the organizational goals set by the board of directors and senior management, risk management ensures that the process of identifying, measuring, controlling/monitoring and reviewing is implemented throughout the whole risk management process (Bank of International Settlements, u.d.). In addition, the risks and the management plan should be mitigated and reported to the board.

Further, to ensure that the risk management process is implemented accurately there should be an in-house Chief Risk Officer (CRO). CRO safeguards that all risks are strategically assessed within the corporate risk policy, the business is responding properly to new risks and challenges, and provides advice on sensitive risk issues for suitable decision-making (Picket, 2013, p.76-77). Overall, the CRO’s task is to make sure that an effective internal control system is being implemented to manage the risks effectively. However, barriers such as insufficient strength of the process, inadequate risk managers, inappropriate risk analysis and
unsatisfactory attitude towards risk should be understood by the CRO when assessing the risk management plan (Carter & Chinyio, 2012). This is why it is worth to make ongoing improvement on the way banks manage the risk effectively.

2.2 Operational Risk

Besides credit, liquidity and market, operational risk is the other significant risk in banks. These risks are all interconnected to each other, but for the purpose of this thesis the focus is only on operational risks and how they should be managed. Thus, in case of the absence of operating loss as the biggest loss, all other types of failures are considerably less important. Further, many banks have collapsed and experienced financial problem because of ineffective risk management system in general and ORM in particular, especially important this issue became after GFC. Although, the last financial crisis has been generally characterized as a liquidity crisis, operational risk and its factors played a significant role in crisis length and severity (Jongh & Vuuren, 2013). Therefore, the need to explore the concept of operational risk has increased significantly.

During long period of time, operational risk remained a residual category for uncertainties which was difficult to identify and measure in traditional ways (Power, 2005). In the last decade, increasing interest to operational risk caused the release of standards and frameworks. The general definition of operational risk provided by such frameworks is “the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events”. This definition includes legal risk, but excludes reputational risk (BCBS, 2006, p.144). SFSA addresses the diversity of institutions by providing alternative approaches for calculating operational risk capital requirements concerning different levels of risk-sensitivity and sophistication (Finansinspektionen Regulatory Code a).

There are only few detailed studies done by scholars on operational risk and its factors. For the purpose of this thesis, the literature on operational risk aspects are to a major extent based on a study done by Jarrow in 2008. Authors believe this study provided the most detailed information on each factor, but some additional sources are used for a better understanding of some of the concepts. Below is the definition of each concept:
People risk
People risk includes the risk of loss associated with errors and illegal actions of Bank’s employees, their lack of qualifications, improper organization of work in the bank, etc. People risk can also involve human error, insufficient training and management of personnel, lack of segregation of duties, lack of honesty and integrity.

Process risk
Process risk is the risk of loss associated with errors during operations and calculations, accounting, reporting, pricing, etc. The risk includes the implementation of transactions on all stages and other aspects of managing a business such as products and services risk, imperfect control system and lack of security or tough security.

System and technology risk
Implementation of IT into business environment brings challenges to workflow, procedures and policies, which in turn can lead to risks. Thus, risks associated with IT cannot be considered independently, but only in connection with people, process and other related risks (Fheili, 2011). IT system problems caused by viruses, cyber-attacks and other failures lead to significant problems which influence the whole organization. Therefore, system and technology risk can be classified as the risks of losses due to imperfect technology used in the banks, e.g. the lack of systems capacity, their inadequacy in relation to the ongoing operations, inappropriate data processing methods, poor quality or the inadequacy of data used. Using effective IT analysis and management together with providing IT security will lead to successful functioning of the entire risk management system (Culbertson, 2004).

External risk
External risk is the risk of loss associated with changes in the environment in which the bank operates. Changes in legislation, politics, economics, and the risk of external physical interference in organization’s activities are other major external risks.
Though reputational risk has been specifically excluded from definition of operational risk provided by Basel Committee on Banking Supervision (BCBS) it has effects on the other factors of the operational risk and helps with creating a more clear and specified map to identify these risks (Xifra & Ordeix, 2009). Reputational risk is a potential outcome of operational risk management and important while it has got too little attention during a long period of time. Therefore it is important to define this risk as below:

**Reputational risk**

Reputational risk is a major risk for all organizations which needs to be considered together with other major risks namely operational (The Chartered Institute of Management Accountants, 2007). Reputational risk can be defined as “the range of possible gains and losses in reputational capital for a given firm” (Forbrun, Gardber & Barnett, 2000).

**2.2.1 Operational Risk Management (ORM)**

Considering general steps of risk management, ORM further focuses on the issues that at first sight are not financial, but may result in actual financial loss. Thus, operational loss can occur at all levels of organization, from board of directors till colluding groups of people (Jongh et. al., 2013). Since 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), internal operational risks are usually closely linked to the activity of a particular bank. Operational loss databases need to be quite detailed and include comprehensive and clear classification of all internal weaknesses while adopting changes (Apatchioae, 2014).
After some rogue trading events in the late 90’s BCBS developed Basel frameworks for managing and providing regulatory options in the field of operational risk (Wiley, 2013, p.4). Although GFC was basically a liquidity crisis, it also increased the attentions to ORM. According to Andersen et.al., (2012) the main causes of the financial crisis were severe violations regarding ORM, mostly due to the lack of attention to its processes. Study by Cagan (2009) shows that size of operational risk losses in 2008, the peak of crisis, was four times higher than in 2007. Also, operational losses did not change a lot in frequency, but significantly increased in severity, meaning that their financial impact became heavier during the crisis (Esterhuysen, 2010). Thereby, the financial crisis consequences showed that the cause of problems in the management of systemic risk has become vulnerable in ORM (Jobst, 2010). In addition, appearance of new and more advanced IT systems with higher security increased attention to ORM (Jongh et al., 2013). Aparenthioae (2014) stressed that the imperfection of bank’s IT and data architecture to support the risk management on the appropriate level, was one of the greatest lessons learned from the GFC for managing operational risks.

After the crisis, ORM was still facing many challenges under uncertainties and decision makers faced problems with managing risks related to bank failures. Also, a rather new aspect which appeared in risk management after financial crisis was changing in investor behavior towards risk (McLaughin, 2013). Rapidly changing regulatory frameworks was another reason for the challenges in ORM processes (Beans, 2010). To conclude, ORM processes were far from perfect during and after the crisis and therefore led to great operational losses and problems. Thus, more attention should be paid to assessment, modeling and management of ORM.

2.3 Internal Control

From past and currently internal control failures take a common place in the banks resulting in huge financial losses. Internal control is an important part of operational risk management and provides a reasonable assurance to achieve the objectives of the organization. Together with an effective risk governance, reliability of financial reporting (COSO, 2013), compliance with applicable laws and regulations, implementation of internal control system can be achieved. In addition, Chernobai, Jorion & Yu (2011) stressed that most of the operational risks come from consequences of weak internal control. Here there is literature review on national and international standards, monitoring and reporting regulations, and risk governance. These are
believed to be the most common internal control frameworks that are applicable at nearly all banks.

2.3.1 International and National Risk Regulations and Frameworks

During the formation of risk management as a recognizable field and at the same time challenges with understanding the term “risk” differently, there was a need to establish standards for the possibility of a unified interpretation by all the practitioners (Simister, 2000). The role of supervision, capital requirements and bank regulation in financial system was highlighted with severity of GFC, both globally and at country level. Further, regulations can administer the impacts of economic crisis but at the same time excessive regulation can lead to a decline in profitability of banks and make their activities more limited (Mulbert & Wilhelm, 2011). Therefore, to manage risks better and for having a proper control mechanism throughout the organization, some international and national frameworks should be implemented. These frameworks are presented below:

The Second Basel Accord (Basel II) is a well-established standard that was initially issued by the BCBS in 2004. Generally, Basel II is intended to facilitate standards for measuring operational risks in banks. It also necessitates the consideration of standards by the board of directors and financial institutions in order to establish a strong risk [management] culture (BCBS, 2003). Further, Basel II reflects improvements in risk management and enables banks to plan and foresee future risky events (Collier, 2009). Though Basel II is widely accepted and established in bank practice since its release, there are some negative opinions on the application of it. The standard came into effect in 2008 in Europe (McAleer, Jimenez-Martind & Perez-Amaralda, 2013).

In 2010, as a response to the crisis, BCBS issued The Third Basel Accord (Basel III), a new regulatory standard on bank market liquidity risk, capital adequacy and stress testing (BCBS, 2011). The main aim of Basel III is to intensify the existing regulatory capital requirements in order to improve strength and flexibility of international banking system by enhancing the regulation and risk management of the banks (Keefe & Pfleiderer, 2012).

Early evidence of implementation of Basel III by international banks shows good progress especially in increasing the quality and quantity of capital. Also, Basel III framework has the necessary directions for improving overall financial stability rather than stability of each financial institution (Schwerter, 2011). The main benefit of Basel III framework is to create a
new internal control level, which can be cut in time of financial distress, provides banks with more flexibility and more financial stability (ibid).

However, because Basel III is just a modified version of Basel II, many drawbacks can occur. Since it does not change risk-weighting, Basel III effectively doubles down on Basel II (Rajiv, 2010). Thus as one can expect, this framework reduces foreseeable risks, but not unforeseeable risks (ibid). Also, implementation of Basel III raised many discussions, since the application of this standard made changes to some parameters of capital requirements needed for operational risk management (Grundberg-Wolodarski, 2012).

The Committee of Sponsoring Organizations (COSO) Internal Control - Integrated framework was introduced in 2004. The framework defines internal control as “process, affected by an entity’s board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting and compliance” (COSO, 2013). Effectiveness of internal control according to this model is based on five integrative components namely control environment, risk assessment, control activities, information and communication, and monitoring activities (ibid).

Despite the undeniable advantages of COSO internal control framework, there are some criticisms about it. COSO framework is just a highly abstract conceptual framework that does not define control objectives at a specific level enough for detailed audit tests (Rubino & Vitolla, 2014). Yet, it is still the one that most of banks are using to define their internal control processes.

Besides Basel II, Basel III and COSO as international frameworks, Swedish banks have to comply with the rules and regulations which are introduced by SFSA. SFSA’s main role is to ensure systematic stability in the financial system and to supervise, authorize and monitor all companies with businesses in Sweden (Finansinspektionen Official website). Further, SFSA regulations protect customer interests.

According to SFSA, monitoring and control in banks must be performed continuously and in case of possible material deviations. Unreasonable results during trade should be analyzed to see whether these have been caused by mistakes, irregularities or other occurrences in banks’ operations (FFFS 2014:1). Further, all accounts should be reviewed and reconciled on an ongoing basis; the value of its net positions and the transactions that give rise to them should
be verified. Lastly, limits for accounts’ positions should be determined and regularly followed up and controlled at least on a quarterly basis (ibid).

Specifically on ORM, SFSA published a new set of regulations in second quarter of 2014. The new regulation contains rules on all aspects of ORM such as risk appetite, control, risk governance, reporting, risk indicators and measurements (Finansinspektionen’s Regulatory Code b). Further, the new set of SFSA’s regulations address most risk areas of operational risk such as IT and information security (FFFS 2014:5) containing the accessibility, security and confidentiality risks within the area. There is also directing to risk management, risk control, and the implementation of Three Lines of Defence (3LoD) in the document (Finansinspektionen’s Regulatory Code a).

Concerning positive sides and drawbacks, these frameworks and regulations, national and international, are the most common ones used by Swedish banks for managing operational risks.

2.3.2 Risk Reporting

Together with risk regulations and internal control frameworks, risk reporting plays an important role in risk management process. Financial Stability Board (2014) stated that risk reporting is one of the major components of disclosure in banking industry and after GFC risk disclosures became one of the effective tools for avoiding possible bank crises. Barakat and Hussainey (2013) discussed the impact of bank governance, regulation and supervision on risk reporting quality within operational risks. To be better prepared for a possible crisis, it is not only sufficient to improve the quality of risk management structure but also to embed the risk governance with CEO and CRO who report directly to the board of directors (Aebi et al., 2011). Further, Howell (2014) mentioned that effective risk reporting can be achieved by close collaboration between board of directors and senior management where management not only provides facts, but explains key performance indicators. This is in line with SFSA’s suggestion on risk reporting as well (FFFS 2014:4). Also, the shift from traditional/manual reporting procedures to the use of digital technologies allows distribution of more qualitative information and gives more time for analysis which in turn increases the quality of reporting (Howell, 2014).
2.3.3 The Three Lines of Defence (3LoD)

According to Doughty (2011) strategic implementation of the 3LoD is the first principle of risk governance framework for providing effective operational risk management. At the present time, the 3LoD is the standard model to prevent risk and manage uncertainty in banks. The 3 LoD consist of three levels as following:

The first line includes business frontline personnel. Their main task is to understand their roles and responsibilities and to perform these correctly and fully on a day-to-day basis (Doughty, 2011). In addition, in the first line, employees need to apply internal controls to treat the risk associated with their tasks. Besides the frontline employees, the risk management committee monitors and builds the department’s day-to-day risk environment (Doughty, 2011).

The second line consists of supervision functions which includes compliance and risk control. The responsibilities of these line employees include participating in the business unit risk committees, reviewing risk reports and validating compliance to the risk management control requirements (Doughty, 2011). It is important to note here that questions related to risk culture, risk appetite, risk budget, risk monitoring and reporting, risk governance approach and the risk management framework are mostly directed to the second line of defence (ISACA, 2011).

Lastly, the third line consists of internal auditors who independently and objectively take the role of consultants and add value to the organization. They help the organization to achieve its goals by bringing in a systematic approach that provides effective risk management and control procedures to the business (KPMG, 2009). There is higher level of independency in this line comparing to the second line.

It has been noticed, that companies without a well-established 3LoD are in danger of experiencing challenges such as gaps in risk coverage, increased costs and value reductions, confusion, less control and ineffective risk oversight (EY, u.d.). However, there is little evidence on the drawbacks and challenges when applying this model in the literature and more research needs to be done on the matter. For better understanding of the framework, the model below is presented:
2.3.4 Stress Test

While concerns about bank capitalization, especially among larger banks and financial institutions increased during GFC, a stress test was used as analysis or simulation tool to determine the ability of the bank to deal with possible economic crisis. Bank of International Settlements (2009) defined stress testing as a category which “represents assessments of a bank’s financial status when faced with the occurrence of several/severe (yet plausible) risk events which might affect its financial performance, capital volume and even existence”. Thus, stress-testing was suggested as the most proper method to measure organization’s preparedness towards risk in time of economic development (Negrila, 2010). It is important to note that since the introduction of stress testing during financial crisis, significant improvement to the quality and level of capital in large banks has been observed (Furlong, 2011). Thus, based on studies, it can be concluded that stress test is an important and necessary control tool for checking bank financial and capital stability.

2.4 Summary of Literature

Concerning the increased importance of operational risks, the above literature review was conducted in order to identify the basic principles of such risks challenges and how they are managed at banks. Likelihood and financial impact therefore affect how such risks are perceived as critical. For better managing such risks principles on adequate risk governance
and internal control should be implemented by banks. Therefore, they need to comply national and international regulations, take an attempt to build positions within the 3LoD and apply stress-testing annually to have control on how operational risks are managed. Operational risks should be reported periodically to senior management and the board of directors who set the risk appetite and risk culture of the organization for better internal control and management of operational risks together with other types of risk. The period prior to, during and after the recent crisis was of interest to collect literature. The literature provided here, although quite new, but it included all aspects of operational risk management that are implemented in practice at banks and it considers the changes to the economy especially in the past few years. The model below gives a better understanding of how all the concepts are related for better operational risk management:

![Figure 4. Summary Model](image-url)
3. Methodology

3.1 Research Approach

The aim of this study is to determine how risk management, internal control and risk governance have been organized to handle operational risks and how operational risk management has improved in recent years. Because of anonymity, this study is done on one of four biggest Swedish banks, named Kungliga Kapital Banken, hereafter KKB. Therefore, as Jankowicz (2000) says it is a case study as the focus is on a set of issues in a single organization and a unit of the organization: the Group Operational Risk Management (hereafter The Group). Further, the issues were explored in a 7-year period, from 2007 to 2014.

This thesis continues the process by adopting a qualitative research method. According to Bryman and Bell (2007) qualitative method provides detailed and in-depth analysis, observation on different aspects and has more flexibility. Therefore, the authors believe this approach is the most suitable for this research. In order to make further analysis and to answer research question, data has been collected from documents available from KKB such as annual reports and documents available on the bank’s website together with additional external sources. Also, the interviews with eligible employees of KKB took place in April 2015 to assess the data collected and to gather more updated information.

3.2 Motivation of Case Selection

3.2.1 KKB - One of the four largest retail banks in Sweden

KKB is one of the four largest retail banks in Sweden with more than eight million private and company customers at national and international level. Being one of the biggest retail banks, KKB is an indicator of the financial economy of the country. Like any other business the bank faces various internal and external risks. One of the priority objectives in the bank's strategy is to keep the risk at a low level (KKB Official Website). Therefore, it is important to assess such risks and be ready to manage them for long-term survival of the business and country's economy. Together, with liquidity risks during the crisis period KKB faced challenges with operational risks which were one of the reasons this bank was chosen for research. Further, concerning operational risk challenges that KKB like the other 3 major banks in Sweden faces, it was interesting to know what actions have been taken to improve operational risk management. Though operational risk challenges are not specified to KKB,
but number of reported risks on media each year on this bank was another reason which convinced the authors to investigate on how these risks are managed at the bank.

In addition to their home market in Sweden, KKB also has major operations in some Eastern European countries. In order to support customers KKB has also operations in both Nordic and Western Europe (KKB Risk Report, 2014). Thus, operating internationally makes KKB more specific and even more interesting to study in terms of operational risk management. Due to the fact that KKB is one of the major Swedish banks, this research and its findings will contribute to more efficient practice within operational risk management in other large banks in Sweden. Some issues related to operational risk management are common within banks and this study will provide a further understanding of how they can be managed considering control and risk governance frameworks.

By the request of respondents and with authors’ understanding of topic’s sensitivity in this study, the name of the bank was changed to a fictitious name as KKB.

3.3 Data Collection

In order to get better understanding and make a complete picture of operational risk management in KKB, authors gathered data from 2007 till 2014, where 2007 was the first year KKB’s risk report was published online for all stakeholders. Therefore, it was interesting to see how changes affected operational risks until the time this thesis was written. The last report published was from the fiscal year of 2014. During this seven-year period, the GFC was a major incident affecting banks including KKB. Although a liquidity risk, but authors believe the crisis affected how operational risks were managed at the bank. This is in line with literature review done by researchers during and after the crisis.

The primary data was collected through the interviews. By collecting data through interviews, authors gained a detailed understanding of how KKB continuously deals with and manages operational risks. This information was then taken into consideration when analyzing the data considering control and risk governance frameworks. Secondary data was gathered through documents available at KKB’s website such as the annual reports, risk reports and additional documents related to the matter.
3.3.1 Data Documentation

Data collected through interviews were recorded with permission of the interviewees. The records were then listened carefully by authors a day after each interview in order to not to lose the sense of the topic for a reliable analysis.

3.2.2 Respondents

For having better access to the information that is mostly internal, the authors focused on finding key personnel in the bank dealing with operational risk management. One face-to-face interview and two phone interviews with employees on managerial level dealing with the subject took place on April 2015 to gain better knowledge on the topic. This also provided different viewpoints on the matter to get a clear picture of the risk management approach.

3.3.3 Interviews

The primary source for collecting data for this research was one semi-formal structured face-to-face and two phone interviews with key personnel at KKB. Generally, face-to-face interviews are preferable because more possible details can be captured by asking additional questions outside of the interview structure. Therefore, in order to make recognition of the potential significance of the context and the depth of meaning, a face-to-face interview was conducted. Thus, face-to-face interviews are optimal for developing closer relationship with the respondent and providing better clarification of questions which subsequently leads to obtain more information (Marin & Marin, 1989).

Due to the geographical distance, two of the interviews were done through phone. Phone interview provides additional flexibility and opportunity to make as many notes as necessary during the conversation without becoming self-conscious (Sturges & Hanrahan, 2004). But it should not be forgotten that it does not provide the flexibility of asking as many additional questions as possible like a face-to-face interview. For each interview, questionnaire with open-ended questions was intended. Also, during the conversations, additional questions were asked for the flow of conversation and for better understanding of each matter. Since the key personnel were at different positions, two sets of questionnaires were made to gather the best possible information. The aim was to have all topics covered during the conversation. The main goal of the interviews based on questionnaire A (Appendix A) were to collect data on operational risk management, control, their relationship and get an overview of how main risks threatening the business internally were being managed. Questionnaire B (Appendix B)
was intended to collect information on IT system risk connected to operational risk management. Through secondary data collection, it became apparent that KKB was facing many challenges when it came to managing IT risks, therefore, the interview took place to address solely this aspect.

The interview guideline was based on issues originated from the literature on risk management, operational risk management and internal control frameworks, in order to collect the sufficient data to answer the research question. Three interviews were planned and occurred. The reason that authors did not continue with more interviews was that after second interview the answers were almost similar to each other not providing more additional data for this research. This is believed to be due to the sensitivity of topic and that interviewees were careful to not reveal data that otherwise should not be published.

Before the interviews, the authors established close contact with interviewees through e-mail, so the physical and phone interviews were suggested by either parties rather than e-mail Q&A. The authors were really careful in interpretation of data analysis after each interview.

By the request of interviewees, their personal information is anonymous. Also, none of the interviewees’ exact positions at KKB were mentioned. Interviewee X was at the operational risk managerial position at KKB headquarter in Stockholm. Interviewee Y was also at managerial position dealing with the subject responsible for south of Sweden. Interviewee Z was at managerial position dealing specifically with IT system risk within operational risk management in Stockholm. All interviewees had insights from the Eastern European region as well.

3.3.4 KKB Seminar

KKB’s internal seminar was used as an additional way to gather necessary information in order to get even deeper understanding of the subject. Thus, due to high level of confidentiality on detailed information about operational risk from the bank, authors were able to attend a two-day internal seminar placed at KKB’s headquarter in Stockholm, Sweden. Seminar attendants were employees of KKB from different divisions and branches including the Eastern European countries. Through two intensive seminar days, more data was gathered that were otherwise difficult to obtain through secondary sources. Presentations and discussions at this two-day seminar were a great source of data giving the opportunity to get better and deeper understanding of research study topic and helped to create more specific
questionnaire for the interviews. Detailed information on how risks are actually managed at KKB was gained through this seminar in addition to getting a better view on how internal control and risk governance affect managing operational risks. This information is not published in much details in annual and risk reports as they were discussed at the seminar among internal employees. Some employees were working at first or second line of defence and had full insight on how the risk governance and internal control frameworks are affecting operational risk management. Therefore, data gathered from the seminar were really helpful for authors to get a better understanding of operational risk management in practice. Data gathered were then compared with literature on the topic for framing the analysis.

3.3.5 Archive Searching

As one of the largest retail banks in Sweden, there is much information available on KKB website in form of documents, annual and risk reports. When looking through annual and risk reports and for the purpose of thesis the focus was on gathering data about operational risks the bank faced each year, how they were managed from operational risk management point of view and how internal control and risk governance affected managing such risks. Also, it was important to understand KKB’s future plans for the upcoming years to prevent the bank from same operational risks they faced in a specific year. In addition the authors used external sources such as the national media and internet sources to gather data on risks threatening the bank and risk management approaches during this period. It was interesting to know how media reflected some issues related to operational risk management and how they assessed the effects of such risks on KKB’s customers. Thus, all possible information concerning operational risk management at KKB that were useful for research was reviewed and analyzed.

3.4 Data Analysis

There are many theoretical frameworks and analytical techniques for analyzing semi-structured interview to obtain the most objective and reliable data. Data collected from the interviews were reviewed and transcribed by both authors the day after to gain correct data understanding and interpretation. In order to reduce researcher error, collected data were clustered into the appropriate concepts from the literature review as they were summarized in summary model, Figure 4, page 16.

The main purpose was to limit the extent to which authors could be influenced by the view of interviewees and to get “original” interpretation. Finally, in order to sum up the analysis of the
received information, detailed analytical summary was done. For the analysis of data, Figure 1 (Risk Impact- Likelihood Matrix) on page 5 and Figure 2 (Operational Risks) on page 9 were used to see if the data collected are in line with what literature has suggested on the subject. It should be noted here that not all aspects of each factor of operational risk were considered for analysis. The focus was on the ones that were mostly mentioned through data collection.

### 3.5 Data Quality

According to Bryman and Bell (2007) reliability is “the consistency or constancy of a measuring instrument”. Thus, in order to get maximum reliability of findings, questionnaires used in the interviews were drawn up in such way as to avoid possible double interpretation.

Despite the different definitions of validity in literature the main factor uniting this concept is the relationship between data and conclusion (Gillham, 2000). Thus, the main focus in achieving validity in qualitative research must be to reduce the gap between reality and representation, data and conclusion (Golafshani, 2003). Authors tried to achieve validity by using the researcher's bias, one throughout the study to maintain ethical standards and principles, performing collection, interpretation and analysis of data as clear and as impartially as possible (Merriam, 1998).

In comparison to quantitative data, interpretation of qualitative data is a more difficult task. Therefore, authors analyzed data separately, discussed results together and then wrote analysis and conclusion. However, other interpretations still can take place. Although qualitative research is often criticized for its lack of generalizability with its definition as “ability to apply the results of research conducted on a sample of a population to a broader population” (Babbie, 1995), Maxwell (2005) considers that a small number of participants severely limits the ability of the researcher to understand the diversity and heterogeneity that exaggerate the uniformity of the phenomenon or impose a single model that only fits a part of the population. Though, the results are specific to KKB because of particular organizational structure and risk management system, but the findings can be used for better understanding of what might be the same situation for other banks.
4. Empirical Framework

4.1 KKB’s Approach towards ORM

Published in 2004, by 2007 Basel II came into effect in Swedish banks, resulted in KKB releasing their first ever risk report (KKB Risk report, 2007). Basel II was fully applicable by the beginning of 2008 (Interviewee X). Risk responsibilities were then given to each of bank’s business units and branches. Risks were evaluated on the basis of their likelihood and financial consequences of each event. The Group then also presented their risk management model. Below there is an insight of this model:

![KKB Risk Model](implementation.png)

Risk management at KKB is organized in a way that it does not exceed board’s risk appetite (Interviewee X and KKB Seminar). Today, KKB’s risk management is based on the 3LoD, clear goals and strategies, policies, an effective operational structure, and national and international risk reporting regulations (KKB Official Website). Further, as expected the board establishes reporting requirements and monitors the risk and capital situation on a regular basis to meet the regulatory requirements (KKB Risk report, 2007). KKB also makes sure that periodical meetings with shareholders, board of directors, CEO, business areas and different group functions take place regularly to mitigate risk and control plans all over the organization.
4.1.1 What are the operational risks at KKB?

By 2007 and with publishing their first risk report, KKB also defined a model for operational risks as follow:

![Operational Risk Table]

It was said that the Group’s overall operational risk was identified low in 2007 (KKB Annual report, 2007). This was in line with their ever goal to keep this risk at a low level. KKB then defined operational risk as the loss related to inadequate or failed internal processes related to each aspect of this risk (people, processes, IT system, and external) (KKB Risk report, 2007). External source of risks affecting operational risks in this year were mostly related to card fraud reported on national media that affected quite many customers.

By the time the GFC got severe, the situation of operational risks also changed for KKB. The first and second quarter reports from 2008 showed operational risks at their normal level. But at the peak of the crisis, the level of operational risk was reported higher than normal. Interviewee X mentioned that incorrect registered funds requested by SFSA were one of the main reasons for these risks. Eastern European countries were exposed to steep operational risks affected from external environment (Interviewee X), which affected the overall operational risks at KKB. It should not be forgotten here that the need for IT system improvements also raised the level of risks (KKB Risk report, 2008).

In 2009, due to the crisis, the economic situation in countries where the bank had operations was severely impacted. From operational risk point of view, this year was a turbulent year.
Political instability in some of the Eastern European countries, the new influenza and external fraud were major sources of operational risks (KKB Risk report, 2009).

Though the Group’s operational risk level was still high, the bank’s overall risk level decreased in 2010 (KKB Annual report, 2010). The main reasons for high operational risk were mostly among Swedish IT infrastructure and external risks mainly from the Eastern European units. The IT system risk was due to a comprehensive disruption including Automated Teller Machines (ATM), card system and internet banking (KKB Risk report, 2010). Natural disasters such as the volcano in Iceland and some terrorist attacks threatening KKB had limited impacts on the bank in 2010 (ibid).

While in 2011 almost all banks were in their post-crisis, the debt crisis in Europe increased and influenced the overall political risk. Although KKB’s overall operational risk decreased, it was still ranked higher than normal (KKB Annual report, 2011). It was believed that the reason behind was the organizational changes aimed to increase the efficiency of workflow and clarify roles and responsibilities within different units. Moreover, IT system disruptions continued as they were in previous years. Overall phishing attacks on individual customer retail increased, mostly through scams on social networks or by attacking customers’ unprotected personal computers (KKB Risk report, 2011). It should not be forgotten that there were some challenges for KKB with implementation of new external regulations.

After a challenging year in 2011, in 2012 KKB did their best to decrease the overall risk level. Yet, the operational risk level was still considered higher than normal just as it was in 2011 (KKB Annual report, 2012). Though the overall operational risk level from IT side decreased, there were still some major incidents reported on media with the threat of cyber-crime attacks and fake e-mails to bank customers.

In 2013, the main drivers of operational risk continued to be IT and system risk related to life-cycle issues in legacy systems. External fraud attempts against the bank’s customers decreased comparing to previous year while external threats were still on high level (KKB Risk report, 2013). These were because of customers growing access to bank’s services via internet and other electronic channels (ibid). From the data presented in the risk report in 2013, the risk appetite was unclear to public, there were no clear overview of internal changes and there were no quantitative measures on operational risk (KKB Seminar).
During 2014, KKB’s operational risk level remained at low level and no major operational loss occurred though card fraud remained one of the critical threats to the bank (KKB Risk report, 2014).

Talking about overall risks, Interviewee Y and Z named IT risk as the most critical operational risk for the bank. As Interviewee Z mentioned, the challenge for the bank is that they need to both satisfy the business and customers by developing IT systems and maintain their services in the most cost-effective way. Further Interviewee Z mentioned that since society is in the era of digitalization, it is difficult to provide the service that all customers want via internet and telephone banking. Also, there is the risk of accessibility, competency, security and development that are challenging within the IT system risk for KKB. Cyber-attacks and security breaches are increasing and have a high threat level to the bank even though KKB has not yet experienced any with severe disruptions (Interviewee Z). Replying to the question about IT system failures that affect customers and published on media Interviewee Z mentions:

“I would say that our services work well often. We have a complex IT-environment (some modern and some older services) and a high change frequency which results in incidents occurring. We suffer incidents with minor impact (not affecting customers) and incidents with major impact resulting in disruptions for our customers. When we have severe disruptions for example disruption in the Internet bank we of course have headlines in the national media because most customers are affected.”

While all interviewees mentioned IT system risk as the most critical risk, interviewee X added the changes in regulations as another emerging risk for the bank, so it was in line with this information mentioned in risk and capital adequacy reports. Regulations from EU and at national level force banks to change and adapt their operations to these new regulations. Therefore, these changes will entail operational risks (Interviewee X). Also, the new sets of regulations might result in the bank performing the reporting process manually, but this is not always the case (ibid).

Taking a look at other aspects of operational risk, people’s risk is another important part of it. Thus, Interviewees X and Y mentioned that people’s risk such as human errors are reported on a case-by-case basis. Further, from KKB’s Seminar it became apparent that human errors that are costing the bank more than SEK 25000 are the ones reported. These are mainly the
incidents that affect customers and may have regulatory impact on the bank operations. People’s risk is usually mentioned together with other types of operational risk, as Interviewee X put it forward.

4.1.2 What were the ORM approaches during 2007-2014?

From the very beginning of defining operational risk it became apparent for the bank that measuring such risks were challenging as they were not easily quantifiable comparing to market and credit risk. These risks were mostly intangible to the bank. In 2009 self-assessment tests were the most important risk identification mean and around 200 tests were conducted through different business units (KKB Risk report, 2009).

From 2010 till end of 2012, the bank took effective actions such as changes in organizational structures to better define the roles and responsibilities aiming at better work flow. The goal for these years was to ensure the stabilization of IT operations and accessibility through Internet Bank and ATMs. The amount of incidents linked to changes decreased. The Product Approval Process (PAP) which was implemented in 2009 across The Group and modified in 2011 has also been effective in mitigating risks related to changes (KKB Risk report, 2014). It has been said in KKB’s Seminar that with implementation of PAP quality assurance at The Group was increased and resulted in more satisfied customers. With PAP the bank tried to prevent disruptions in services provided to customers. In addition, operational efficiency was achieved to some extent (KKB Seminar).

KKB’s attempts to stabilize operations on Internet Bank and Telephone Bank that started from 2012 continued with resulting in 59% less incidents in the first 9 months of 2013 comparing to the same period of the previous year. In addition, the maintenance time to fix the problems decreased by 49% (KKB Risk report, 2013). Also, during 2013, KKB created centralized procedures for mapping the risk process together with the key control activities within organization. Further, during 2013, a common risk-based planning process was established, which was refined in 2014 to ensure relevance of risk management and risk control activities and to enable resource allocation within The Group’s risk function over time (KKB Risk report, 2014). Later in the year, KKB improved its performance in terms of handling changes within the business.

Further, in 2014, KKB’s risk appetite for operational risks was refined. They also formalized monitoring and reporting procedures (KKB Risk report, 2014). Though it should not be
forgotten that as customers’ internet access to bank services such as mobile and internet banking are increasing, managing the threat of cyber-attacks are always high on agenda. It was mentioned in KKB’s Risk report from 2014 that criminals had access to multiple channels to commit fraud. However, the losses in this area were close to zero thanks to active risk mitigation (ibid).

4.1.3 What are the continuous ORM approaches?

Generally, like other banks, KKB takes a wide range of measures, from electronic security and active shutdown of fictitious and infected websites to provide information directly to the customers. Part of operational risk management is done when new products, services and IT systems are developed or significant changes are made, while the impact on all stakeholders is taken into consideration. Measures to further safeguard IT operations and accessibility through the Internet Bank, Telephone Bank and ATMs are continuing (KKB Risk report, 2014). All these are included in an incident management plan that covers crime, error, service disability, human errors and etc. Incident management limits the impact of risks on The Group’s services, discovers the incident, responses, reports, assesses and mitigate the related risks (KKB Seminar).

Larger losses of material significance are rare, and KKB seeks to reduce the likelihood of these through risk management frameworks, namely Business Continuity Management (BCM). Therefore they can maintain ready for events that could cause financial losses, reputational damage or impact the availability of the services. Within BCM organization’s stakeholders, reputation and brand will be protected and more value is added to the business (KKB Seminar).

The risk management maturity assessment tool was introduced in 2014 and is a scorecard used to assess business’ risk management maturity level in various topics. A high risk-management maturity level within the business indicates a strong risk culture and risk awareness – which in turn reduces the threat of unforeseen losses and keeps business assets secure and safe (KKB Risk report, 2014).

KKB on a regular basis, each year conducts stress tests to identify the potential effects of possible negative scenario, to estimate the effects of tail events and to assess whether the capital level is satisfactory. Therefore, readiness to possible breaches in the market increases (ibid). The Group conducts scenario-based simulations and stress tests at least once a year to
ensure efficient use of capital, meets minimum legal capital requirements and maintains access to capital markets even under adverse market conditions (KKB Annual report, 2014). Further, there is increased focus on performing SFSA stress tests annually for economic stability and to assess capital evaluation in the bank. Recent stress tests together with SFSA’s report showed that KKB has stable position and can remain resilient in case of a possible crisis.

What is obviously been problematic for KKB under operational risk management is various IT system risks related to the IT infrastructure they face several times every year.

4.1.4 What were the internal control procedures at KKB?

In 2009 after several incidents from Eastern European region, KKB was forced to strengthen risk governance, risk management and internal controls, and the role of CRO was introduced. Further, in 2009, political instabilities were assessed and appropriate actions were implemented (KKB Risk report, 2009). As always, an analysis of The Group’s risk level was quarterly reported to the board for risk regulations on the overall business and continued in the following years. Regulations from the board include KKB’s risk tolerance, basic principles, description of responsibilities and methods to manage operational risks (KKB Annual report, 2009).

In order to further improve the internal control, in 2013, a framework for Internal Control of Financial Reporting (ICFR) was implemented. The framework’s aim was to continuously evaluate and develop internal control for all that is influencing the profit/loss account (KKB Annual Report, 2013 and Interviewee X).

Although intangible, internal control at KKB is based on organization’s structure, policy and instructions defined by the board of directors (KKB Official Website). As expected and according to Interviewee X internal control plays a really important role for the bank and is a developing area in The Group. Financial reporting together with control self-assessment tools were mentioned as other internal control approaches by Interviewee Z. In addition, KKB is using internal control frameworks to control risks such as the COSO framework although there are not so many apparent references to the use of the framework (Interviewee X). Interviewee Z, mentioned that new internal control frameworks are based on the development of the existing ones such as COSO.
It should not be forgotten that one main risk governance framework that has been implemented to the bank is the 3LoD model easing the control process over risk management. Interviewee Y made some arguments on the use of model and how it can weaken effective internal control processes. According to Interviewee Y, sharing responsibilities in line with 3LoD makes the flow of control and communication difficult. Lacking proper control then results in increasing operational risks for the bank and failure in managing such risks is for sure costly to the bank (KKB Seminar). Further, on the challenges with implementation of 3LoD, Interviewee X mentioned:

“Historically the distribution of roles and responsibilities of management and risk control has been unclear and something what we have worked on to define and clarify. Today we have a very clear separation of roles and responsibilities between first and second line. What happens is that second line more and more fulfills the tasks historically performed by third line as first line assumes ownership for risk management. That means that collaboration between risk management, risk control, compliance and audit becomes ever more important to avoid duplication of efforts and hence the implementation of a risk based planning process”.

To be able to better manage operational risks and to have proper internal control over the organization, it is important for KKB to apply different regulations into their day-to-day business. Interviewees Y and Z mentioned that regulations are always good no matter what and will help KKB to better handle the risks, implement a better internal control process and allocate capital. Interviewee X also mentioned that:

“There are many regulators issuing different regulations, and sometimes those different regulations have not been aligned and can post contradictory or overlap requirements. It is imperative to understand that regulators issue regulations and institutions are required to make sure that the business is organized in accordance with those regulations.”

To summarize, it can be said from the data collected in this section that IT system risk and external fraud are the major risks KKB is facing that are identified by the authors. IT system risks have high likelihood and will increase the overall operational risks with high financial impacts on the bank. Reporting regulations, people’s risk and cyber-attacks to some extent have been challenging for KKB, but did not result in major operational losses and any
incidents related to these were not published on the national media. Political issues at Eastern European countries were a threat to the bank as well during the period studied for this thesis.

4.2 Analysis

4.2.1 Operational Risk

The release of Basel II caused increasing interest to operational risk (BSBC, 2006), respectively, the implementation of Basel II in 2008 at KKB turned operational risk into a significant part of risk management process. Though the goal was to constantly keep the level of operational risk at a low level, KKB faced serious challenges in this area. Although the financial crisis was mainly a liquidity crisis, but it affected operational risk level (Jongh et al., 2013) and KKB’s situation with respect to operational risk confirms this judgment. Thus, operational risk level not only increased in 2008 but remained high for a few years till 2011, inconsistent with KKB’s goal to keep this group of risks at a low level. This resulted in KKB applying changes on how operational risks are managed in the bank. Further, measuring operational risks in comparison to other types of risk (market and credit) is not an easy task since such risks are not easily quantifiable from data provided and all are not tangible.

Before moving forward to all aspects of operational risk it should be mentioned here that the literature on external risk connected to operational risk mostly mentions natural disasters and terrorism as major external risk (Jongh et al., 2013). At KKB, such risks in 2009 and 2010 played really limited role in increasing the overall operational risk. Therefore, The Group included other areas in the external risk affecting the overall risk level. The effects of politics on this risk group can easily be seen as KKB decided to decrease the level of operations in some Eastern European countries as challenges within these countries increased.

Looking more deeply into different aspects of operational risk (people, processes, IT systems, and external), it became apparent that while managing the other aspects, KKB put IT infrastructure in focus. External risks related to operational risk are of importance as well. Some part of the IT infrastructure environment is quite old, causing costly problems for the bank from time to time affecting customers. Being one of the biggest retail banks in Sweden, gaining high attention from national media, KKB is facing issues with losing their reputation among their main stakeholders, customers. In the digitalization era most of customers are shifting from the retail services to the use of internet banking which causes significant problems with access, system stability and security at KKB. For example, the card fraud
related to both IT system and external risk was a source of operational loss for the bank in the past few years. All these named risks support Fheili (2011) statement that IT risks should be considered in connection with people, process and external risks.

Even though, there have not been any major issues concerning cyber-attacks, they have happened and they might happen in future which will then result in customers to be worried about being scammed by fraudsters. Again the reputation of bank is in danger. One might say that reputation is not included in the definition of operational risk provided by BCBS (2006), so it does not affect this risk group, but evidences from data collected showed that KKB categorizes loss of reputation as an external risk, therefore, it does affect the overall operational risk level.

Noticeable is the fact that people’s risk such as human errors in manual reporting or material misstatements are concerned as a threat and are reported only when the resulted loss is more than SEK 25000.

All in all, although actions were taken when the bank identified such risks, IT system risks, external fraud and risk of losing reputation at KKB can be categorized as major/critical risks with high likelihood and high financial impact. This is the subjective interpretation of authors from the collected data. The authors did not look at all areas of operational risk as presented by KKB, but these were the ones that were mentioned often in the secondary and primary data collected. Thus, it’s important to stress here that more attention should be paid to the named risks in order to minimize their impact on the overall business.

4.2.2 Operational Risk Management

Risk appetite and risk culture were named among the baseline of risk management by literature and regulators (Roeschmann, 2014 & EY, 2013). Communication with all business areas and those performing tasks within 3LoD has continuously helped KKB to clarify its risk appetite. A proper definition of these two factors should include the tolerance for changes and KKB needs to consider this continuously. It was seen from the data that although not really clear, but the board at KKB has taken these two terms into consideration when approving the operational risk management plans. In addition to risk appetite and risk culture, complying with regulations are of importance. Legislations issued by SFSA along with international standards such as Basel II, Basel III and COSO are the most used regulations among Swedish banks and financial institutions including KKB.
Further, KKB has applied the use of PAP into its operational risk management procedures for documenting all the changes related to identifying and managing risks. It is believed that the application of PAP has resulted in KKB better managing risks arising from changes due to new set of regulations. It is also important for KKB to develop the incident management plans and BCM along with changes in all areas of operational risk.

Reporting and monitoring are also other significant part of the operational risk management process (Financial Stability Board, 2014) and it was stressed that many operational risks occur because of problems caused by process failures in monitoring and reporting (Dunnet, Levy & Simoes, 2005). Although not publicizing all risk management processes, especially those related to operational risks in annual ad risk reports, these reports are available to the internal staff and are done according to available frameworks. Reporting and monitoring internally are in line with what regulations and literature are suggesting for the financial institutions (FFFS 2014:4 & Howell, 2014). But, the data showed that these reports are prepared manually from time to time increasing the level of operational risks, and management approaches should be taken into consideration. Although, the excessive new regulations are one of the reasons for manual processes, KKB should be able to adapt itself to these changes in the fastest way to decrease risk of material misstatements. Risk management maturity assessment tool is believed to be helpful. So, these findings support Howell (2014) who stated that shifting to digital technologies will give more time for analysis which in turn will increase the reporting quality.

4.2.3 Risk Governance and Internal Control

Internal control became much more important part of operational risk management in the recent years. Internal control in KKB is performed in line with suggested frameworks, standards and regulations on financial institutions. ICFR is also important part of internal control at KKB which helps with improvements in overall quality of risk reporting. In addition, KKB considers components of COSO framework to implement internal controls which help with better managing the risks (COSO, 2013). Though, there were critics to COSO and that other standards might be applicable to financial institutions; KKB still bases the internal control on COSO components. This is in line with what other financial institutions are doing (EY, 2013).

3LoD has been characterized in literature as one of the most efficient risk governance models and have a detailed structure on internal control (Doughty, 2011). KKB also uses this model
as well in its operational risk management process. Although, interviews showed that 3LoD has helped with clarifying responsibilities related to managing risks, it is believed by the authors that the model is challenging. This is inconsistent with literature that did not show any issues with application of this model. Empirical findings further showed that challenges mainly appear in the blurred boundaries between tasks in all three lines of controls, which in a way overlap with each other. Also, communication and control difficulties can occur because of sharing responsibilities according to this model. Therefore, risk management process takes a longer time and becomes even more costly and to some extent inefficient.

Stress testing is a control tool used in banking sector for assessing bank’s vulnerability and to illustrate the impact of key risk factors on the bank (Bank of International Settlements, 2009). The Group conducts internal and external stress test on regular basis as one of the significant risk measurement tools and data from the recent years showed that KKB will face less challenges if a major economic downturn happens.

To summarize, it can be said that internal control has been implemented in accordance with COSO components, 3LoD model and stress testing. Despite some criticism in the literature, COSO model is the most appropriate and effective in the field of banking activities and the fact that KKB as one of the largest uses this framework highlights its advantages. While business practices show 3LoD as the most proper way to govern the business and internal control procedures, we argued that there are drawbacks and imperfections in its structure, namely with regards to the allocation of responsibilities at all three levels of control. Stress test remains as one of the effective tools to determine the bank stability and its flexibility to manage risks. It is therefore, apparent that risk governance and internal control frameworks such as national and international regulations, have improved the way operational risks are managed, but there is still room for more improvements.

The figure below is an interpretation of authors’ point of view on KKB’s most critical risks that should be taken into consideration. From data it became obvious that the probabilities of some risks are more than other ones, namely IT system risks and external fraud. The outcome of these two risks, reputational risk, is then another critical risk for the bank. Together, if not managed properly they have high financial impacts on the bank and are critical (as marked in the red area). Other risks in the matrix, comparing to these three, then have either less probability or have less financial impact on the bank. Again it should be mentioned that these
risks were the ones were mentioned most often in the data collected and the authors did not study all areas of operational risks as defined by KKB.

The risk assessment matrix can be used for the fiscal year of 2015. Risks are dynamic and with KKB’s attempts to manage these risks continuously, the situation presented in this matrix can change from time to time.

Figure 7. KKB Risk Assessment Matrix
5. Conclusion

5.1 Operational Risk Management and Internal Control

The purpose of this study was to examine how operational risk management, after identifying critical risks, has improved by applying risk governance, internal control frameworks and regulations. In this thesis operational risk management and its factors were described based on a case study on one of the largest retail banks in Sweden – KKB. The critical risks within the operational risk framework presented by data on KKB were identified, namely the IT system risk, reputational risk and external card fraud, assessed and analyzed with the use of literature on the subject. These risks are the ones that happen regularly and are believed by authors that have high financial impacts on the bank. As a result, the bank has started paying more attention and takes considerations on better managing these risks by introducing more efficient procedures on managing operational risks at the organizational level.

Improvements in IT system affect the overall level of operational risks (internal and external) and the level of security. Financial impacts will then decrease as well. With media’s continuous attention to every operational failure, mostly those related to external card fraud, cyber-attacks and IT environment, the bank should be careful on how their reputation is affected. The financial losses of damaged reputation for one of the largest retail banks cannot easily be replaced. Further, our findings show the differences between what has been suggested about reputational risk in literature and reality. It has been noticed that reputational risk is an important part of operational risk management when it comes to banks and it needs to be placed under external risks.

In addition, the findings show that the recent crisis affected the level of operational risks to some extent. Therefore, KKB faced challenges within internal control frameworks applicable at the bank and was forced to apply changes. Internal control therefore played an important role in how banks started to imply new risk management procedures to their operations. Basel II and Basel III introduced by BCBS and COSO framework at an international level together with national regulations, namely SFSA, changed how internal control was practiced at KKB after the crisis. These frameworks were really helpful in improving how operational risks were managed at the bank. New set of regulations make the bank to manually continue the requested reporting processes which increases the human errors within the people risk. Although challenging, these regulations helped KKB with managing operational risks in a
more efficient way than they did before. Further, reports showed how the implementation of 3LoD has helped with identifying a better internal control environment at banks though the model lacks strong scientific background and it has drawbacks when implemented. Incident management plans, BCM, PAP and stress-testing are among regular internal control activities which help KKB to manage operational risks even more efficiently.

This thesis’ findings confirm that even though ORM has been improved a lot, still many problems occur at the bank increasing the level of operational risks. Therefore, it is important for KKB to continue applying changes and improvement plans to manage these risks while concerning a unified internal control framework. The authors believe that results of this study can be helpful for other banks with same size and operations especially when it comes to IT system risks, external and reputational risks. Regulations and internal control issues can be applicable to all banks as they are unified and risk management approaches suggested by this study would be helpful for reducing the risks of these factors. A clearer picture from this thesis’ findings about operational risk management can benefit academia researches and make them more interested to proceed further in this topic.

5.2 Future Research

By conducting this study a subjective understanding of critical operational risks and their impact on managing this risk group within a Swedish bank was studied. Operational risk management improvements were made in the field of ORM during last seven years. Therefore, the future research can be conducted by studying other areas of operational risk that were not studied here. Other variant for further study could be a comparison between two banks/financial institutions concerning ORM factors within risk governance and internal control frameworks. Further, it will be interesting to solely study the impacts of 3LoD on risk management model in practice and identify the drawbacks over a period of time. All these possible future studies can bring a great benefit from a practical and academia point of view. An internship in the bank within the Group Operational Risk Management would be an interesting approach to gather more information for a future study on the topic.

5.3 Limitations

This study was limited to only one bank and a specific period of time prior to, during and after the recent financial crisis. Further it was limited to the use of published annual, risk reports of the bank and there is not so much information from internal sources. Since KKB has a certain
structure and some aspects of operational risk are specified for this bank, findings can be
generalized to only some extent for possible use in other correlated banks especially when it
comes to IT environment, external fraud and reputation. Also, the interpretation of gathered
primary data can depend on authors’ subjective reflection.
References


EY. 2013. “Remarking financial services: Risk management five years after the crisis”.

FFFS 2014:1. *Finansinspektionen’s Regulations and General Guidelines regarding governance, risk management and control at credit institutions.*


FFFS 2014:5. *Finansinspektionen’s Regulations and General Guidelines regarding information security, IT operations and deposit systems.*


Appendix A

Questionnaire A

1. Can you give us short background information on yourself and your job at KKB?

2. How do you define KKB’s risk appetite on operational risks?

3. Could you elaborate more on KKB’s risk culture concerning operational risks?

4. How does KKB assess the people risk? For example human errors?

5. How do you assess the role of internal control within the Group operational risk?

6. How do you assess the importance of communication in risk management?

7. Concerning the issues that KKB has faced during and after the Global Financial Crisis, how do you assess your reputation among your main shareholders, mainly the customers?

8. Economy is changing fast therefore regulations change quickly to safeguard the economy. To what extent do you think the national and international regulations threaten KKB’s operational risk?

9. How often and from which area, within operational risk, does KKB categorize risks as critical?

10. Are all risks a threat to KKB or is there a possibility of a risk being an opportunity for further business development?

11. Are there any drawbacks on the implementation of 3LoD?

12. What is the threat of economic situation at Eastern European countries on the overall Group in 2015?

13. If a financial crisis happens in 2015. Do you think KKB’s is ready to handle it from the operational risk side?
Appendix B

Questionnaire B

1. Can you tell us shorty about yourself and your position at KKB?
2. How you can describe IT system works in general (challenges, success factors, future planes)?
3. What IT system risks are usually occurring? Which of them you can define as a critical threat to KKB?
4. How long the general maintenance work (omfattande underhållsarbete) takes and what influence it has on banks clients?
5. How often IT system risks must be reported to the management?
6. Do security breaches happen? If yes, how often?
7. How can you describe the current situation with such external risks as cyber threats and external fraud against the bank’s customers?
8. What about system instability or failure? How often does it happen?
9. Concerning the IT system failures that happen every now and then, how do you assess KKB’s reputation among customers?
10. Is there any system of internal control for IT system risks?
11. To what extent to do you think the overall regulations on risk management influence IT system risks?
12. How do you predict the situation of IT system risk for 2015?