INSTITUTO
UNIVERSITÁRIO
DE LISBOA

The impact of Artificial Intelligence in Operational Risk Management

Maria Carolina Pereira de Carvalho

MSc in Business Administration

Supervisors:

PhD Rui Alexandre Henrique Gonçalves, Invited Assistant Professor,

ISCTE Business School

PhD Renato Lopes da Costa, Assistant Professor,

ISCTE Business School

July, 2021

BUSINESS
SCHOOL

Department of Marketing, Strategy and Operations

The impact of Artificial Intelligence in Operational Risk Management

Maria Carolina Pereira de Carvalho

MSc in Business Administration

Supervisors:

PhD Rui Alexandre Henrique Gonçalves, Invited Assistant Professor,

ISCTE Business School

PhD Renato Lopes da Costa, Assistant Professor,

ISCTE Business School

July, 2021

Acknowledgements

The conclusion of this master's degree means the conclusion of a very important chapter of my life. A long and not always easy journey, where I could discover my skills and my passions at a professional level. This would not be possible without the amazing people that surround me, to whom I would like to thank:

To my parents and brother, for entirely believing in me and for the absolute support in all the adventures, which would not be possible without them.

To my grandparents, for the values they instilled in me, for the pure love and unconditional encouragement, for being my inspiration.

To Tomás, for the motivation, the love and endless patience on the best and worst days.

To Hugo, Teresa and Inês, for all the crucial help throughout my academic path.

To all my family, friends and colleagues, for their help, ideas, suggestions and support that gave me strength and guidance over these months.

To the interviewees, for their availability to share with me their experiences and opinions, which were essential for this dissertation.

To my supervisor, Renato Lopes da Costa, for the sharing of knowledge along this path.

To the co-supervisor, Professor Doctor Rui Alexandre Henriques Gonçalves, for the support and fundamental motivation, as well as for the contagious sharing of knowledge in the area of operational risk.

Abstract

Within the risk areas, Operational Risk is the furthermost unexplored area of all. Considering the last decades and the several economic crises that Europe and the world have experienced, Operational Risk is a rising area and companies are slowly starting to realize that the more they invest on the control of Operational risks, the less profits they lose. Artificial Intelligence is the critical topic of the century, being wide enough to cover almost every area imaginable, bringing easy, cheaper and more precise ways of doing all sort of tasks. This research reflects the progresses made by companies from various sector of activity in the implementation of Artificial Intelligence technologies in the mitigation and control of Operational Risks.

The qualitative research completed by the analysis of a set of interviews revealed the deficiency of investment around Operational Risk, as well as the absence of knowledge and information concerning the progress on the Artificial Intelligence technologies applicable to Operational Risk controls. Obstacles as the lack of human resources capabilities and prioritising other sectors were shared by the interviewees as an impediment to the application of AI systems in OpRisk. Companies must develop and invest in the Operational Risk departments, considering the existing Artificial Intelligence solutions that allow for the maturation and improvement of the control of these risks and, therefore, allows to mitigate losses that occur from them.

Key Words:

Operational Risk, Artificial Intelligence, Automation

Resumo

Dentro das áreas de risco, o Risco Operacional é a área mais inexplorada de todas. Tendo em conta as últimas décadas e as várias crises económicas que a Europa e o mundo viveram, o Risco Operacional é uma área em ascensão e as empresas aos poucos começam a perceber que quanto mais investem no seu controlo, menores são as perdas. A Inteligência Artificial é o tópico crítico do século, sendo ampla o suficiente para cobrir quase todas as áreas imagináveis, e trazendo soluções fáceis, económicas e mais precisas para todos os tipos de tarefas. Esta pesquisa estuda os avanços feitos por empresas de diversos setores de atividade na aplicação de tecnologias de Inteligência Artificial na mitigação e controlo de Riscos Operacionais.

A pesquisa qualitativa realizada pela análise de um conjunto de entrevistas revelou a deficiência de investimento na área de Risco Operacional, bem como a ausência de conhecimento e informação sobre o avanço das tecnologias de Inteligência Artificial aplicáveis aos controlos de Risco Operacional. Obstáculos como a falta de qualificação de recursos humanos e priorização de outros setores foram partilhados pelos entrevistados como impedimentos à aplicação destes sistemas. Neste sentido, as empresas devem ponderar o investimento nos departamentos de Risco Operacional, considerando as existentes soluções de Inteligência Artificial que permitem maturar e aperfeiçoar o controlo destes riscos e como consequência, mitigar perdas que ocorram dos mesmos.

Palavras-Chave:

Risco Operacional, Inteligência Artificial, Automatização

Index

Index of Figures

Index of Tables

Glossary

OpRisk – Operational Risk

AI – Artificial Intelligence

IT – Information Technology

ML – Machine Learning

DL – Deep Learning

ANN - Artificial Neural Network

BIA - Basic Indicator Approach

TSA - Standardized Approach

AMA - Advanced Measurement Approach

LDA - Loss Distribution Approach

DT - Decision Trees

AIRMS - Artificial Intelligent Risk Management System

HR – Human Resources

Introduction

Theme Framework

As firms and banks progressively expand their operations, more complex these become and to sustain the business there is one thing that should be taken into consideration: the risks. Human beings are constantly facing situations that require decision-making processes, each with different implications and therefore with different levels of risk. The association between risk and reward is part of human common sense, and for that reason the reflection of risks is a decisive factor in any choice process, from the simplest things to the more complex ones. Despite the controversial nature of the following statement, it is important to consider that the best decision is not necessarily the one that minimizes the risk, but the one that gives a better result for a certain degree of risk that one is willing to take. According to Drucker (2014), there are a lot of different types of business risks such as the financial risk, strategic risk, compliance risk, between many others. In this investigation I will focus on the Operational Risk.

The awareness of this type of risk began throughout the 90's and is now being heavily explored and enriched. Operational Risk is commonly known as the risk resulting from the inadequacy or failure of both external events or internal processes, that could result in gain or lost earnings. Thus, it is a risk associated to all activity domains, that can be presented through many forms such as frauds, human error, IT failures or natural catastrophes. (Drucker, 2014; Diehl, 2014)

Although this subject appears relatively new, this investigation also tackles one of the most critical topics of the 21st century: Artificial Intelligence. The very beginning of AI cannot be defined, but it was certainly during the Second World War and due to Alan Turing that the topic became relevant. Since that, the concept of AI had an immeasurable evolution, but the foundations remained the same, so we can consider that Artificial intelligence is the set of techniques that aim to simulate human cognition and intelligence in robots, computers, or other machines to perform tasks that are naturally assigned to humans. (Haenlein, M., & Kaplan, A. ,2019; Calo, 2017).

Objectives of the dissertation

Recently, the world started making progresses in merging these two matters, implementing the advances of AI in the Operational Risk Management in order to make this last one more

effective. While there is an extensive research in Operational Risk and specially in Artificial Intelligence, not many researchers took into consideration the merge of both topics. Understanding the progresses in these two areas and the result of this merge became the main objective to develop this topic, so this investigation aims to further explore this literature gap, with the final purpose of understanding in what way the technological advances regarding Artificial Intelligence can impact the Operational Risk Management.

With this being said, this dissertation will focus on three main questions:

Q1: What are the success factors of implementing Artificial Intelligence in Operational Risk Management?

Q2: Which are the possible down-sides of implementing Artificial Intelligence in Operational Risk Management?

Q3: Which are the main drivers of success or unsuccess of the application of Artificial Intelligence in Operational Risk Management? Is it worth the application?

To further explore these research questions, I will conduct a literature review, followed by the theoretical approach and methodology analysis. Then, the results are gathered and followed by the discussion and analysis. Lastly, I will take the final conclusions, aiming to get clarifications on the questions defined in the beginning of the dissertation.

Chapter 1 - Literature Review

1.1 Artificial Intelligence

1.1.1 Concept of Artificial Intelligence, Machine Learning and Deep Learning

Artificial Intelligence, or AI shorten, is not a new topic. Actually, it is present in our daily lives maybe more than we even realize. In the following paragraphs we will try to get to know a bit more about its roots and its subsets.

To talk about AI we should probably go back until the 40s, then the well-known English mathematician Alan Turing developed a code breaking machine called The Bombe for the British government, able to decipher the Enigma code used by the German Army during the Second World War. The machine did what no mathematician could do at the time – it broke the apparently unbreakable code and showed the possibility of intelligence beyond the human brain. This machine was considered the first working computer (Haenlein & Kaplan, 2019).

From that historical event was born the article "Computational Machinery and Intelligence", also written by Alan Turing, where he described how to create and test intelligence in machines. This article is still in our days a benchmark to identify intelligence in an artificial system (Haenlein & Kaplan, 2019). Turing's work was continued by John Von Neumann, whos' major contribution was the idea that computers should follow the logic of the human brain and should be designed as so. Due to many other contributions in the middle of the 20th century machines were already able to solution algorithms (Shabbir & Anwer, 2018).

In our days there are countless definitions of AI: Shabir & Anwer (2018) describe it as the property of machines, computer programs and systems that enable the creation of human functions, such as solving problems, draw conclusions and make decisions. Nadikattu (2019) thinks of it as the capability that machines can have to complete complex tasks that usually would require human knowledge. He describes it as an electronic form of technology that does not require human power. Jakhar & Kaur (2020) shortly consider AI as the incorporation of human intelligence into machines and systems.

Important is to understand that AI machines are able to learn from trends, experiences, tendencies and practices of human behaviours, gather data, scrutinize, observe and carry out processes with, sometimes, higher accuracy in less than humans can (Nadikattu, 2019).

An easy way to understand AI's process is to think in the A→B logic, known as supervised learning, in which input data (A) is used to generate a comeback (B). This process of input A and output B have already transformed many industries, as Ng (2016) predicted. These A→B systems improved rapidly and are commonly built with a technology called deep learning, a technology that was directly inspired by the brain. This system has only one inconvenience, it requires a vast amount of data in order to give enough examples to the system so that AI can unravel the A→B relationship (Ng, 2016).

Around the topic of Artificial Intelligence two more terminologies emerge among academics: machine learning and deep learning. AI generally refers to a field of computer science dedicated to creating systems that perform tasks that usually require human intelligence (Jakhar & Kaur, 2019).

Machine learning is a subsection of AI, which includes all the approaches that allow machines to learn from data without being unambiguously programmed. ML aim to train machines based on data and algorithms. The algorithm is a set of explicit instructions that a computer can run, capable of learning from data itself. The treated data is used by the computers and machines to make assumptions and choices. It is a technique to put AI into action, using the algorithms to minimize errors and maximize efficiency on their predictions (Jakhar & Kaur, 2019).

Furthermore, Deep Learning is a subset of Machine Learning that combines computational models and algorithms that together emulate the construction of the biological neural networks of the human brain, therefore these are commonly referred as artificial neural networks. When this ANN receives new information, it immediately stabs comparisons to previously known data to take conclusions (Jakhar & Kaur, 2019).

The advances in this area of studies have greatly increased the ability to learn, think, develop reasoning and solve problems. All industries are progressively looking upon the use of AI technology, since the agricultural and manufacturing industries, to the healthcare and government facilities (Nadikattu, 2018). As this technology evolve, so as the human dependences increase towards intellectual machines that use the combination of various technologies to understand, perceive, sense and predict actions on their own (Shabbir & Anwer, 2018).

1.1.2 Business application of AI

Artificial intelligence, Machine and Deep Learning have become, in the last years, a central focus of innumerable industries such as information technology, e-commerce, healthcare, cybersecurity, logistic, media, marketing, agriculture, arts, military, between many others (Nadikattu, 2016) (Kolbjørnsrud *et al*., 2016).

Artificial Intelligence is changing practices and procedures throughout all industry sectors. Businesswise, it is a revolutionary technology that came to eradicate the traditional practices concerning operating businesses. Unlike in the beginning of this century, business can now be managed from everywhere, from home, from the office or even from the other side of the world (Nadikattu, 2019). As Kolbjørnsrud *et al*. (2016) expected, artificial intelligence will soon be qualified to do the administrative tasks that consume most of managers' time, with a couple of particularities - they will be able to do it faster, better and at a lower cost.

Shabbir & Anwer (2018) considered that the implementation of robotics in business contributes to potentialize various ranges of activities such as customer service, finance, sales and marketing, administration and technical processes in multiple sectors. Should be also considered as an important complement to help and allow people to develop their potential and creativity to the maximum.

So, there is an increasing influence of AI in business applications, with many solutions already implemented and many more being explored. In many sectors machine learning techniques have been proven to perform better than traditional statistical techniques, both in classification and also predictive accuracy (Leo *et al.,* 2019). Thus, it is particularly interesting for this topic to understand the application of Artificial Intelligence in other areas of risk management, such as credit risk management and market risk management.

The specific case of market risk is still an unexplored matter. Aziz & Dowling (2018) define market risk as the risk that emanates from investing, trading, and generally from having exposure to financial markets. Several investigators have researched market risk and volatility from a portfolio or investment risk management perspective. However, from a bank risk management perspective, the papers are still very limited (Leo *et al.,* 2019).

Some authors support that machine learning is particularly suited to stress testing market models to determine inadvertent or emerging risk in trading behaviour. Another area of

focus within the category of market risk is understanding the impact of trading firms on market pricing (Aziz & Dowling, 2018). Arian *et al.* (2020) provide an innovative approach for measuring market risk called Encoded Value-at-Risk or Encoded VaR, which is based on a type of artificial neural network (ANN). It is a multiplicative model that can be used to reproduce market scenarios from a range of historical cross-sectional stock returns, while increasing the signal-to-noise ratio present in the financial data and learning the dependency structure of the market without any assumptions about the joint distribution of stock returns (Arian *et al.*, 2020).

As for the Credit Risk, it is defined by Aziz & Dowling (2018) as the economic loss that emanates from the failure of a counterparty to fulfil its contractual obligations. These authors emphasize the increasing interest by organizations in using AI techniques to enhance credit risk management practices, sometimes due to evidence of incompleteness in the traditional techniques, since credit risk management capabilities can be significantly improved through leveraging AI techniques due to its ability of semantic understanding of unstructured data.

Cheng & Qu (2020) assume that the use of AI in banking reduces significantly the credit risk in the case of Chinese commercial banks. They analyse this thematic pros and cons: First they consider that banks employing emerging technologies contribut to improving bank risk management efficiency and thus reduces bank credit risk. Also, these emerging technologies provide support to the internal governance and internal control, reducing bank credit risk. Secondly, it brings technical risk and regulatory risk, which could increase bank credit risk (Cheng & Qu, 2020). Just as Paul Daugherty, Accenture's chief technology officer once said, *"Artificial intelligence may be the most disturbing technology the world has ever seen since the industrial revolution"*.

1.1.3 The challenges and opportunities of AI

When we talk about AI, we usually refer to the opportunities it brings to our daily lifes and to our jobs, as we'll see below, but first we will think about the main challenges.

The hot topic of the last couple of years is the relation between technology and privacy, or the lack of it. Thus, it is primary to ensure that all technology can provide privacy to consumers. Therefore, it is vital to note that privacy is a key challenge that needs to be attended as AI systems become more sophisticated (Nadikattu, 2019).

Another topic that cannot be ignored or forgotten when we think about the challenges of the rising use of AI is the wave of job displacement that will almost certainly occur as some jobs will undoubtedly be extinguished (Wilson et al., 2017). Haenlein & Kaplan (2019) expect that the escalating use of AI will result in less need for white-collar employees or high-qualified professional jobs.

This job displacement consequence can probably be avoided by some specific regulations that might dodge such an evolution. These regulations can be thought of by demanding that companies spend a certain percentage of the money saved through automation into training employees for new jobs that cannot be automated. But then another problem arises: who will regulate these policies? Since AI is implemented throughout industries, from firms, private individuals to states themselves, international coordination in regulation will be needed after all (Haenlein & Kaplan, 2019).

As Shabbir & Anwer (2018) emphasized, soon another consequence of AI will be the devastating race of arms in fatal autonomous weapons and our full dependence on technology will eventually lead to unemployment issues, social discrimination and power inequality in societies. Thus, the use of robots in a long term will create monumental challenges to the human race. This dependence will raise the issue of the lack of regulation, whether it is needed and, if so, in what way it can be done (Haenlein & Kaplan, 2019).

Haenlein & Kaplan (2019) believe that in the future these regulations will exist through the development of requirements, commonly accepted by the IT industry, that will define the training and testing of AI algorithms, combined with some type of warranty that can be compared to the consumer and safety testing protocols used for physical products (Haenlein & Kaplan, 2019).

After all there are a few challenges, some of them harder that others to overcome, and the media sometimes tend to show an unrealistic picture of the power of this technology developments (Ng, 2016) The propaganda is so extreme that some are suggesting that AI will be the harbinger of disaster for humanity and consider a dystopian world view where machines run the planet (Bini, 2018). But do the challenges outweigh the opportunities?

AI is a world of endless opportunities, which have emerged quickly in the last few years. As Shabbir & Anwer (2018) predicted a couple years ago, robotics as already improved speech, voice, video conferencing and face recognition. Also, in the area of consumer goods and

services, advances in Machine Learning processes have proven to be extremely efficient and profitable when matching consumer demand at reduced prices and higher quality service. The advances in robotics proved to be able to cover both emerging and traditional technologies.

On a business view, AI will certainly revolutionize the way companies compete and grow by generating and developing new and better practices that can lead to a higher business profitability. AI strategies are already used worldwide but they are expected to expand and evolve with a bigger focus on the ethical and moral values (Shabbir & Anwer, 2018).

Despite the expected wave of job displacement, a new opportunity will arise: the creation of many new jobs that will be required to keep up with the technological advances. Wilson *et al.* (2017) divided this in three new job categories: the trainers, the explainers and the sustainers. These jobs will reassure that the tasks performed by the machines are effective, fair, transparent and auditable.

The first category, the Trainers, will be workers who teach the intelligent systems how people's questions with sympathy and depth. Explainers will help provide clarity, which should shorten the gap between business leaders and AI engineers. Lastly, Sustainers will help ensure that the systems are performing the way they were designed to and also that any unexpected concerns are addressed immediately (Wilson *et al.*, 2017).

So, with the jobs that will disappear and the new ones that will emerge, companies will face the need to change their human resources strategy, in order to effectively attract these new professionals who will be in great demand (Wilson et al., 2017). Artificial Intelligent developments will create the need of new skills that include collaboration and communication capabilities, information sharing, testing, learning and decision-making efficiency, and the ability to spread beyond the company for insights (Kolbjørnsrud *et al.*, 2016).

It is unanimous that AI will bring to our daily lifes unique ethical, legal, and philosophical challenges that will need to be addressed, whether it will allow us to enhance our own intelligence, as Raymond Kurzweil from Google once shared, or whether it will lead us into World War III, a concern from Elon Musk, no one could know. The real challenge to the humankind is to admit upcoming evolutions in this fast-moving world while being sufficiently precise to avoid the too much and too quickly overexpansion of AI systems (Haenlein & Kaplan, 2019).

1.2 Operational Risk

1.2.1 Concept of Operational Risk and Operational Risk Management

Operational risks are not as new as the term itself. Human mistakes, fraud, theft, process failures, system errors and external threats, such as natural catastrophes, fires and floods, all of them are considered operational risks and all of them are present for an indefinite time now. However, the relevance of this risks was not much, until globalization have made operational risks more significant than ever before. Nowadays the importance of Operational Risk Management cannot be overemphasized as an inadequate management method can result in unpredictable financial performances and incalculable losses (Weeserik & Spruit, 2018; Fadun & Oye, 2020)

Operational Risk Management is the youngest of the three major risk branches within the financial institutions: Market, Operational and Credit Risks. It became popular after the bankruptcy of the Barings bank in 1995, when a trader caused the fall of a respected institution by placing bets in the Asian markets, keeping these contracts hidden from managers. At the time, these losses where not classified as market neither as credit risks. Then, the term Operational Risk emerged to define situations where such losses could arise. Initially, due to the uncertainly and the unfamiliarity with the term, it had the negative definition of being any risk that not market or credit risk, although that, different from other risks, it is usually not taken to retrieve an expected return. It exists in every organizational activity and their inappropriate management in significant losses (Peters *et al.*, 2016).

Operational risk management is a framework that was made to detect the most critical operational risks to organizations in an appropriate timeframe and effectively report them to all required individuals at different levels of management for them to take the necessary actions. Countless efforts were made toward increasing clarity across organizations on risk events that impact banks' reputation, earnings and performance (Abdul Rahim *et al.*, 2019).

This specific type of management encompasses the mechanisms, tools, policies, procedures and processes to identify, assess, monitor, report and control operational risks. Due to the errors of the past, financial institutions started to prioritize operational risk management to obtain higher capital profitability, better capital allocation, the avoidance of unexpected losses, the improvement of operational efficiency (Giannone, 2018; Abdul Rahim *et al.*, 2019).

According to Drucker (2014), OpRisk Management consists in a continuous and systematic process to identify, analyze, report and monitor the operational risks of an institution in order to Identify opportunities for improvement in business processes, provide support information in strategic decision-making, reduce unexpected events and the respective operating costs, to identify and manage multiple risks by presenting comebacks to different levels of risk and to transform risks into opportunities (Drucker, 2014).

To properly manage operational risks, managers follow the three lines of defense model. This model advocates the assumption that every individual function in an organization has a defined role in risk management in order to reduce the likelihood that a risk goes undetected and thus cause unexpected consequences (Luburić, 2017; Weeserik & Spruit, 2018). This model divides these line defenses by functions that they will perform.

The first line of defense takes care of the operational risk management itself, the second line has the risk management functions and supports and monitors the first line through the development of management framework, the third line is formed by an independent audit committee that assess the complete risk management structure, process and implementation. It supports the proper functioning of both the first and the second line of defense thru internal audit activities (Luburić, 2017; Weeserik & Spruit, 2018).

Thus, the model consists of the follow three pillars: a business line management, an independent corporate operational risk management function and an independent audit assessment. A strong risk culture, good communication and teamwork are vital characteristics to a solid Operational Risk Management (Luburić, 2017).

If well applied, this model achieves efficient results and that's the reason why it's being highly requested and used by financial institutions, since it helps institutions by making them less vulnerable to systemic problems through identifying all the risks that they are exposed to including those that they usually do not have the expertise or experience to manage (Luburić, 2017; Fadun & Oye, 2020)

Additionally, in general an effective process of Operational Risk Management implies six steps accordingly to the authors Carlos & Soares (2018): First of all, identify the risk, thru experience, common sense and specific analytical tools that help identify risks. Second, assess the risk by applying quantitative and qualitative measures to determine the level of risk. The third step is to analyze risk control measures by investigating strategies and tools that help to

reduce risks. After that, the next step is to make control decisions, such as identifying the appropriate decision-maker, as he/she must choose the best control or combination of controls, based on the analysis of the third process. Fifth step is to implement risk controls, for which management must formulate a plan to apply the controls that have been selected and provide the materials and staff necessary to put these measures into practice. Finally, supervise and review, since once the controls are correct, the process must be reassessed periodically to ensure its effectiveness.

1.2.2 Operational Risk Models

Many models have been suggested for modelling OpRisk under the previous Basel agreement, the Basel II regulatory framework. Briefly we can consider two approaches: the top-down approach and the bottom-up approach.

The top-down approach only quantifies OpRisk without attempting to identify the causes of losses. It can include models that rely on some operational risk exposure indicators to track them and can also rely on models that are constructed based on "what-if" scenarios. On the other hand, a bottom-up approach quantifies OpRisk by identifying their internal events and can incorporate models that analyze the frequency and severity of these risks' losses. (Peters et al., 2016) Under these regulatory framework banks could use several methods to calculate operational risks such as: the Basic Indicator Approach, the Standardized Approach and the Advanced Measurement Approach (Peters *et al.*, 2016; Vőneki, 2018)

In brief, under the BIA and the TSA the capital is calculated as simple functions of gross income. These approaches have very rough level of model granularity and are generally classified as simplistic top-down approaches. Under the AMM, banks are allowed to use their own adapted models to estimate the capital. A bank intending to apply this approach should demonstrate the accuracy of the internal models within Basel II specified risk cells relevant to the bank. This has a finer level of granularity, since it's based on a bottom-up approach, that the BIA and the TSA, being more appropriate for a detailed analysis of risk processes in the financial institution. The most widely used AMA is the Loss Distribution Approach (Peters *et al.*, 2016)

As Peters et al. (2016) highlighted, although being valid, it was already demonstrated by studies that the BIA and TSA do not correctly estimate the Operational Risk capital. Alternatively, to these approaches, the current Basel Committee agreement removed all internal

modelling and modelling practice in favor of a new and too simplified one size fits all SMA model (Peters *et al.*, 2016; Vőneki, 2018)

1.2.3 Recommended Practices by the Basel Committee III

Basel II regulations contain the three basic methodologies for measuring the capital to be set aside for operational risks, namely the BIA, the TSA, and the AMA, and summarizes the qualitative and quantitative requirements for use of these methodologies (Vőneki, 2018).

During the financial crisis in US, numerous issues were observed in the Basel II norms. The Basel II norms primarily focuses on ensuring that banks can set aside sufficient capital to cover their risks. The regulations contain three basic methods to measure the capital to be set aside for operational risks, that we analyzed before: the BIA, the TSA and the AMA. But they were unable to protect big banks in the US from the huge and unexpected shocks in 2008. With it comes the urgent need to change the norms and so the Based III norms arise in 2010 (Vőneki, 2018; Boora & Kavita, 2018).

With the Basel III emerged the Standardized Measurement Approach (SMA), supplanting the previous approached, and was then integrated into the European regulations. This new capital measurement approach is based on controlling data and only considers the development of operational loss data in the case of large banks and institutions (Vőneki, 2018).

The main target of the Basel III norms is capital-intensive activities and are expected to improve the stability of the international banking system. The implementation of these new norms is supposed to be integrated progressively and its full implementation was not estimated until 2019 (Boora & Kavita, 2018).

Similar to the AMA before, the new SMA has also triggered a heated debate in professional and academic circles (Vőneki, 2018). Peters *et al.* (2016) seriously criticize the introduction of the SMA saying it does not ensure the stability of the capital requirement, also that it fails to achieve the objective of robust capital estimation stating that it will be neither stable nor robust with worsening robustness as the severity of risks increases. The author also criticizes that it is not appropriately risk-sensitive has the Basel III objectives stabilized, stating that induces risk-taking behaviors, also that is has a reduced risk responsivity and induces risk-taking, furthermore the author emphasizes that it is super-additive and that fails to utilize the range of data sorges or provide risk management insight.

Basel III norms have been regarded as the international regulations for banks to create more resilient banking systems. The implementation of Basel III capital regulations has been drawing more attention all over the world. The regulations provide an opportunity to banks for strengthening their risk management system (Boora & Kavita, 2018).

1.3 AI in Operational Risk

1.3.1 AI in the banking sector

As the banking industry began to understand that the proper planning and sharp decision making will lead to significant growth, there is an increasing need to automate this decision making processes in order to reduce the margin of error and increase productivity. Thus, sooner or later an Artificial Intelligence take over is inevitable, since it is the central technology in many of today's novel applications for every sector, as for example the banking systems that detect attempts of credit card fraud, an AI research-based technology (Smith, 2020).

The continuous focus on solving problems and exploiting opportunities of managers has led financial services workers to adopt intelligent solutions to reduce costs, handle compliance pressures and improve their relationships with clients (Moro *et al*., 2015; Smith, 2020).

Being a competitive industry, banking has developed the ideal scenario for the implementation of AI solutions. It is an attractive field for researchers since it generates a large amount of data where intelligent systems can succeed (Smith, 2020).

1.3.2 Information Systems and Operational Risk

A significant progress of information systems for OpRisk Management had place with the implementation of the Basel II Agreement, with a focus on the construction of data bases of operational risk, development of analytic models and in the structuring of reports to the managers (Gonçalves, 2011). Henriques Gonçalves (2011) mentioned the characteristics the author Chorafas (2011) pointed as a needed evolution for the future of the information systems for OpRisk Management. The author mentioned the importance of a growing need of control, management and real-time response, the capability to analyze and deal with low frequency and high impact situations, also the capability of delivering accurate answers in complex systems.

With increasing requirements, complexity and a growing volume of risks, information systems provide benefits for incorporating risk management activities and improving

performance (Weeserik & Spruit, 2018). According to Weeserik & Spruit (2018), Business Performance Management technologies are believed to provide a solid solution for effective OpRisk Management by offering combined technologies including workflow, data storage, advanced analytics, reporting and dashboards.

1.3.3 The applications of AI in Risk Management – the gap of literature

During the last two decades the application of Artificial Intelligence systems and solutions in finance became a trend, mainly due to the effort made to generate profits thru the forecast of the future movements of the market (Chandrinos *et al*., 2018).

Contrary to previous studies that used Machine Learning algorithms in financial data, recent studies mainly focused on predicting the actual price of stocks and currency pairs or the general direction of them, Chandrinos *et al.* (2018) analysed and achieved the successful application of two machine learning models for risk management purposes. These models are the Decision trees and artificial neural networks. The two models resulted in the development of an artificial intelligent risk management system. AIRMS was applied to the optimized trading strategy in order to recognize which signals will be profitable and which ones will not.

Apart from these, several other studies made a connection between the developments of Intelligence Systems and many financial applications. Milkau & Bott (2018) support that AI has the potential to go beyond and make decisions in situations without predefined solutions. However, this is impossible through the concept of machine reasoning, that doesn't require a vast amount of data but instead is based on previous experiences. This is the prerequisite reasoning to bridge the gap between Artificial Intelligence technologies and Operational Risk Management, a highly unexplored area (Milkau & Bott, 2018).

In the operational risk area, studies have been predominantly focused on fraud and suspicious. transaction detection, as Leo et al. (2019) emphasize. These problems are typically addressed by classification algorithms, and others like gathering analysis, Bayesian networks and classification trees are commonly prominent in the application of machine learning algorithms. Neural networks have also been mentioned to as a very prevalent and prominent technique in credit card fraud detection (Leo *et al.,* 2019).

Thus, the application of AI in OpRisk Management is still widely unknown and unexplored, with few studies analysing and focusing on the matter.

Chapter 2 - Theoretical Approach

Following the Literature Review carried out in the previous chapter of this investigation, and as a result of the various insights presented by the several authors previously mentioned, it was possible to develop 3 research questions that will be address in detail along this chapter.

Having in mind this dissertation has a disruptive nature, the focus of the research took place in papers and authors that, in many ways, discussed the introduction of AI based systems in several branches of management, as well as in other activity sectors.

Beginning by what inspired me to develop the first question, Aziz & Downling (2018) in the paper *AI and Machine Learning for Risk Management* emphasized the costly and time-consuming nature of the risk control and risk management functions, nature that they believed the introduction of AI based systems would help diminish as well as reduce compliance cost base and provide accurate real-time information that will support in predicting risks on a less costly and faster way.

Chen & Qu (2020) focused their research on the use of finance and technology combined to reduce credit risk. In their study they conclude that in Chinese banks the credit risk diminishes with the use of technology, which also improves activities. They predicted that transactions had serious potential to be less expensive, more convenient and more secure. As for the security, Shabbir & Anwer (2018) also sustain the idea that Fintech will potentialize areas such as finance, sales and even administration, by complementing human tasks, and making a huge impact in the prevention and fight against corruption. At the time of the research, they recognized that AI developments were already increasing planning, learning, reasoning and thinking of the machines, that would develop the ability to reproduce human thinking and take decisions previously exclusive to humans. The authors forecast that these technologies would rise competition, drive business profitability while being affordable to any organization.

Following this thought were the authors Milkau & Bott (2018) that supported the idea that AI had the potential to go beyond the task of classification, as machine reasoning would be able to make decisions in situations without predefined solutions. A year after this assumptions Leo et al. (2019) said AI was already adding value in the defence against spammers, blocking malware attacks, theft of data and financial bases.

Converging these predictions, Kolbjørnsrud *et al.* (2016) considered that AI based systems will replace some management functions, doing it better, faster and cheaper. Having all this forecasts in mind, there are several benefits reported from the application of these technologies in management and that is the reason that led to the first research question focused on Operational Risk:

RQ1: What are the success factors of implementing Artificial Intelligence in Operational Risk Management?

On the other hand, aiming to explore both the positive and the negative outcomes of this implementation I focused on the concerns raised by authors as Ng (2016) in the paper *What Artificial Intelligence can and can't do right now?*, where was emphasized that automation would most likely lead to job displacement. This apprehension was also raised by Shabbir & Anwer (2018) and Wilson *et al.* (2017), although the last author considered that, following the job displacement wave, many unique jobs will be created, with new roles and new skills.

Haenlein & Kaplan (2019) discussed about the past, the present and the future of AI and concluded the extreme need of regulation, justifying it by saying that systems can be bias. This is also a concern that Shabbir & Anwer (2018) mentioned, considering the security, lack of regulation and data protection the primarily issue.

Apart from the job displacement and security insecurities, some authors question the limitations and flaws of the AI based systems, like Ng (2016) that considers the biggest disadvantage of automation the huge amount of data it requires, or Wilson et al. (2017) that stated the main failure from AI based machines is the lack of empathy and dept in understanding questions, directly related with the inability to understand emotions.

Other concerns are raised, focused on the performance of companies, where Kolbjørnsrud *et al.* (2016) mentioned her scepticism in the capacity of robots to engage workforce and provide sense of purpose to the worker, which means functions related to drafting strategy should remain unmistakably human. Also, Gonçalves, R.A.H. (2011) assessed the ability of machines to replace human judgement and predicted that AI based systems will redefine Operational Risk companies' strategy and the way they do their daily controls and activities. This author questioned the impact robotization will have in the image markets have of the companies and showed some insecurity regarding fulfilling the needs of the companies.

Identically to the interest in understanding the success factors of the automation of some Operational Risk Management functions, arises the curiosity to understand if the above mentioned concerns the authors lifted are still today a subject of awareness. Thus, the second research question arises, this time focused on the negative side:

RQ2: Which are the possible down-sides of implementing Artificial Intelligence in Operational Risk Management?

In the previous chapter, the Literature Review, we could understand that there are many advantages, disadvantages, challenges or even incompatibilities related with the use of AI based systems in the most diverse areas. The opinions change from investigation to investigation, from one author to another. Authors like Chandrinos *et al.* (2018) considered the use of machine learning models (decision trees & neural networks) to develop AI risk management systems (AIRMS), that they believe will improve negative returns to turn most of the losing years into profitable ones and also to increase even more the already profitable ones. In another paper, Milkau & Bott (2018) said the biggest advantage of machine reasoning would be the instant reaction to new situations, almost a real-time response and adaptative automation.

Aziz & Downling (2018) mentioned the need of training skilled staff to implement new technologies, that will prevent unwarranted risks, unwind dangerous exposures, dynamically adjust risk appetite of the firm based on a system estimate of the broader risk environment. On a very different perspective we have Haenlein & Kaplan (2019) that believe the implementation of AI in a broader way in financial institutions will surely lead to unique legal, ethical and philosophical challenges.

Gonçalves, R.A.H. (2011) predicted the drivers of success of OpRisk Management automation would be wide, but mostly focused on the reduction of losses, upgrade of internal controls performance and development of the OpRisk culture. Although he could not conclude whether the outcome of the use of AI would be mostly positive or negative, so the author suggested a deeper study of the impact of information systems in the area of OpRisk.

Also with that belief are Leo *et al.* (2019) who's secure that ML techniques have already proven to perform better than traditional statistics techniques, both in classification and also in predictive accuracy, but stated that a large number of areas in risk management could significantly benefit from the study of how AI can be applied to address specific problems. They mentioned that research on AI in risk management still falls short, not being as much

explored as other areas of management. At the time of that paper, and still now, there are only few studies that announce pros and cos of the use of AI based systems in Operational Risk Management, one of the areas that will benefit from further studies.

We are aware of the negative impacts of AI and also the benefits it brings in very different areas – but if we had to put it on a scale, what would weigh more? Does the problem of security and data protection weigh more or less for a company than the benefits of automation in the long term, such as reduced costs and increased productivity? Is it worth the application in the OpRisk Management area? This was the main motivation that led me to the third research question:

RQ3: Which are the main drivers of success or unsuccess of the application of Artificial Intelligence in OpRisk Management?

Chapter 3 - Methodology

The present research was divided into four stages, the first stage being the literature review based on bibliographic research and information processing. The second was the theoretical approach, which consisted in transferring the theoretical concepts to the field of observation, building from there the three research questions. In the third phase was carried out the research and collection of data resulting from the interviews and treatment of the respective data, and finally, the fourth step consisted of a qualitative analysis of the data collected from the interviews.

This chapter aims to present the methodology used for the research in order to understand the aspects that guided the research

3.1 Research Model

The methodology chosen for this research have an exploratory and observational base, since OpRisk is a relatively new area, and the topic of Implementation of Artificial Intelligence in Operational Risk Management is not yet well explored. From what I could have access, this is the first investigation to focus on this implementation and do this sort of research to try to understand the advances that has already been made to implement AI based systems in OpRisk, both in Portuguese companies as well as in other foreign companies, a bit all around the world.

Although the reply and accession to the interviews was satisfactory, the conclusions of this investigation must be read carefully and always taking into consideration that it is based in a relatively small sample, which implies the impracticality of making generalizations. This is presented as one of the main limitations of this investigation, together with the gap in the literature review, although both limitations were already predicted in the beginning of this study.

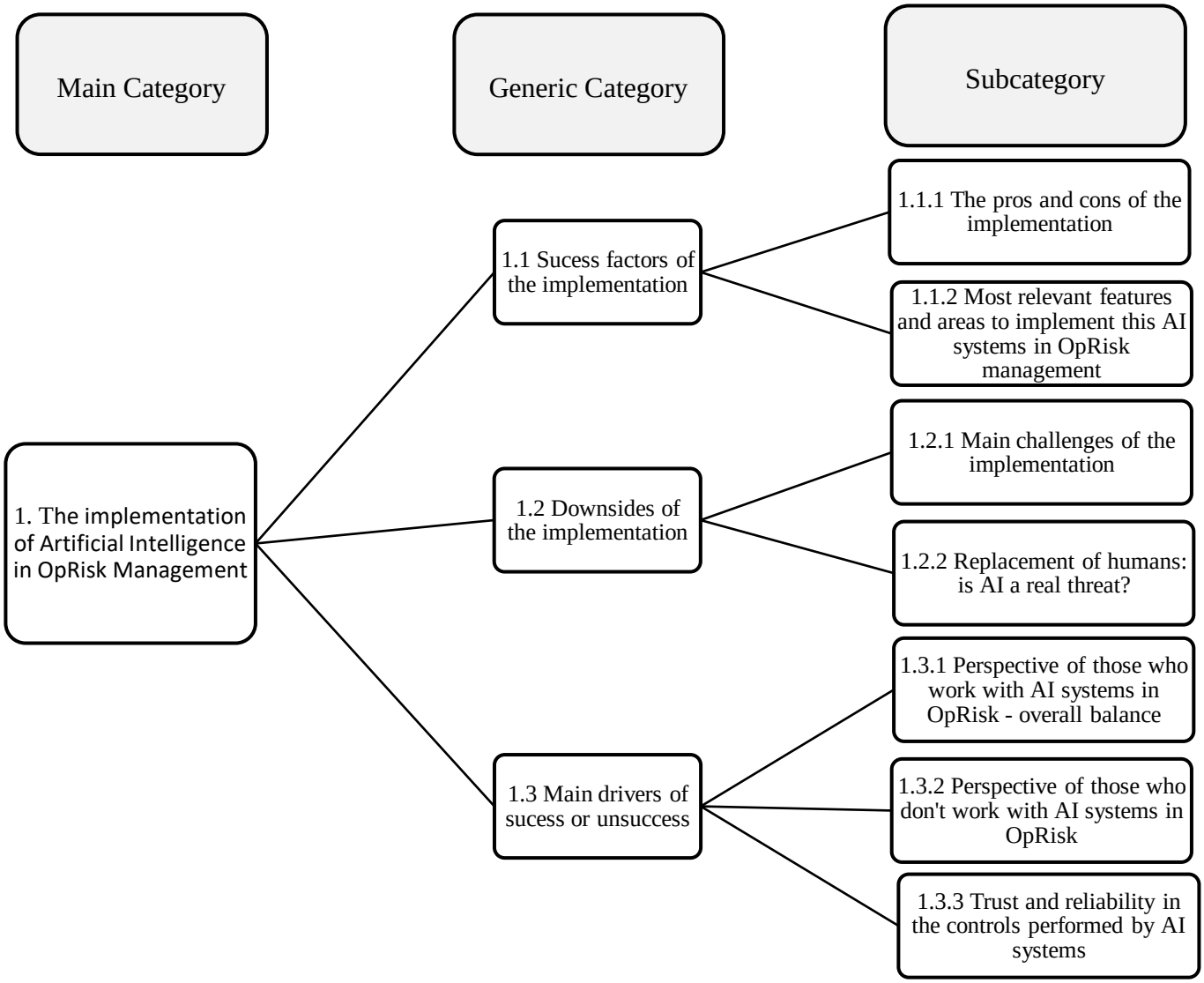
In the following table, Table 1, it is possible to analyze the relationship between the objective of the study, the research questions elaborated in the chapter of the theoretical approach, the respective connection with the literature review previously done and also the methods of data analysis used.

Table 3. 1. 1 – Analysis model that lists the study objectives, research questions, literature review and data analysis method

Objective	Research Questions	Analysis method	Literature Review
Analyze the implementation of Artificial Intelligence in OpRisk Management, addressing the pros and cons and then consider the suitability and the relevance of the automation of the OpRisk process in different sectors	(Q1) What are the success factors of implementing Artificial Intelligence in Operational Risk Management?	Content analysis from MaxQDA system for qualitative analysis of interviews	Cheng & Qu (2020) Leo et al. (2019) Aziz & Dowling (2018) Shabbir & Anwer (2018) Milkau & Bott (2018) Kolbjørnsrud et al. (2016)
	(Q2) Which are the possible down-sides of implementing Artificial Intelligence in Operational Risk Management?		Haenlein & Kaplan (2019) Shabbir & Anwer (2018) Wilson et al. (2017) Kolbjørnsrud et al. (2016) Ng (2016) Gonçalves, R.A.H. (2011)
	(Q3) Which are the main drivers of success or unsuccess of the application of Artificial Intelligence in Operational Risk Management? Is it worth the application?		Leo et al. (2019) Haenlein & Kaplan (2019) Chandrinos et al. (2018) Milkau & Bott (2018) Aziz & Dowling (2018) Gonçalves, R.A.H. (2011)

Source: Elaborated by the author

Table 3. 1. 2 - Categorization and codification of the interview corpus for qualitative analysis



Source: Elaborated by the author

3.1.1 Data collection method

The data collection was carried out through one-to-one semi-structured interviews, which constituted a probabilistic sample.

The choice of the semi-structured interview was based on the idea of not limiting the participants to the script that already channels them to the answers, obtaining more developed answers which allows to achieve diverse types of information that would not be acquired if the interviews were done under a rigid model.

The data collected for this investigation has a primary data character, meaning it was obtained by the investigator directly from reality, being the data source the OpRisk specialists that work in the area, that have knowledge and experience regarding the research questions.

The research was based on a pragmatic or inductive character, which means it does not intend to reach true or false conclusions, but to analyze a set of phenomena, spectacles and facts that allow comparisons to be made and to discover correlations between them.

The data was then treated rigorously, using the qualitative analysis software MAXQDA. MAXQDA is a professional software for qualitative data analysis, which performs the transcription and analysis of interviews that allows to easily categorize relevant information using codes, making the analysis much simpler.

3.1.2 Interview's procedure

One of the most crucial stages of the research was planning the interview and the construction of the respective script.

The interview script is organized into two groups: the first group includes the 4 questions that aim to characterize the sample and the second group includes the remaining questions that aim to achieve the study objective, which is to analyze the implementation of Artificial Intelligence in OpRisk Management, addressing the pros and cons and then consider the suitability and the relevance of the automation of the OpRisk process in different sectors.

The interviewees were contacted through the LinkedIn app, where they were invited to participate in a research that study the areas of Artificial Intelligence and OpRisk, and where the intention was to understand their level of knowledge and experience in automation of Operational Risk controls using intelligent systems, as well as a professional opinion about the advances of AI based systems in the OpRisk area. The interviews were conducted through the Zoom platform. The intention at the time of the contact was not to fully reveal everything that would be covered during the interview so that the interviewees could answer spontaneously, without any previous preparation.

In the beginning of the interviews, it was explained that this was a research for a dissertation to obtain a master's degree in Business Administration. Moreover, it was clarified before the start that the investigation aims to understand the impact of Artificial Intelligence on Operational Risk Management, and for that purpose it would be important to understand the number of companies that have already implemented some automation based in AI to their daily tasks and what was the outcome of that implementation. Lastly, it was also mentioned the

importance of getting to know cases of companies that don't have progresses in this field and try to recognize why, what are the obstacles and if there is a project or an intention to implement this kind of automation in the future.

The interviews were performed from the March 1, 2021 until March 12, 2021, they took around 30 minutes and were all audio recorded, having in mind that in each and all of them it was agreed between both parties that the personal data of the interviewees would be always kept into absolute confidentiality. The decision to stop with the interviews was not taken because of the amount of it, since it is a considerably small sample. The decision accrued from a noticeable loop of answers, which mean that the answers and feedbacks I received where starting to repeat considering the previous interviews. For the data analysis methodology, all the 16 audio interviewees were carefully transcribed and some of them translated to English.

3.2 Sample characterization

This study is constituted by a probabilistic sample, which means the sample individuals were chosen from a specific population. In this case I choose professionals related with Operational Risk, namely team managers, OpRisk analyst and OpRisk advisors.

For the sample characterizations it was taken into account parameters such as the country and the sector of activity they work in, for how long they work in the area of OpRisk and also the kind of functions they perform. Parameters as age and gender were not taken into consideration since the majority of the individuals asked for complete confidentiality and most of them didn't agree in answering those questions. This request for total confidentiality accrues from the area of OpRisk being relatively new and small, which make the identification of these professionals easier if parameters as age and gender were revealed, and also because sometimes the information passed denotes risks that can be created by human errors, made by the company' employees.

The 16 professionals interviewed were in its majority from companies based in Portugal, as you can see below in the Figure 1, which corresponds to about 62,5% of the sample, although it is important to note that the interviewees from Portuguese companies also work with several foreign markets. The remaining interviewees are 6,25% from Spain, 6,25% from Norway, 6,25% from Finland, 6,25% from Denmark, 6,25% from Brazil and 6,25% from Singapore.

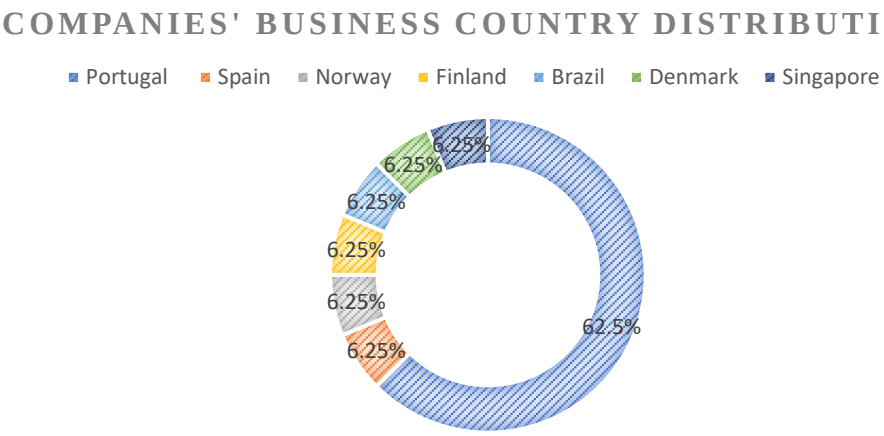


Figure 3.1 - Companies' business country distribution

Source: Elaborated by the author

The interviewees were in its majority from the banking sector (62,5%), the second sector with most representativity was the insurance sector (18,75%), then there were also some specialists in OpRisk from the utilities sector (12,5%) and also from the consulting sector (6,25%). See below the Figure 2.

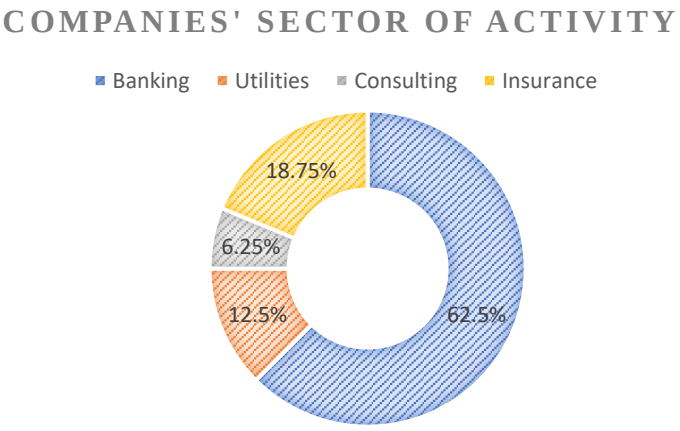


Figure 3.2 - Companies' sector of activity

Source: Elaborated by the author

The interviewees were 56,25% Team Managers, while OpRisk Analysts correspond to 37,50% of the sample and the minority of them are 6,25% of OpRisk Advisors, as you can see presented below in the Figure 3.

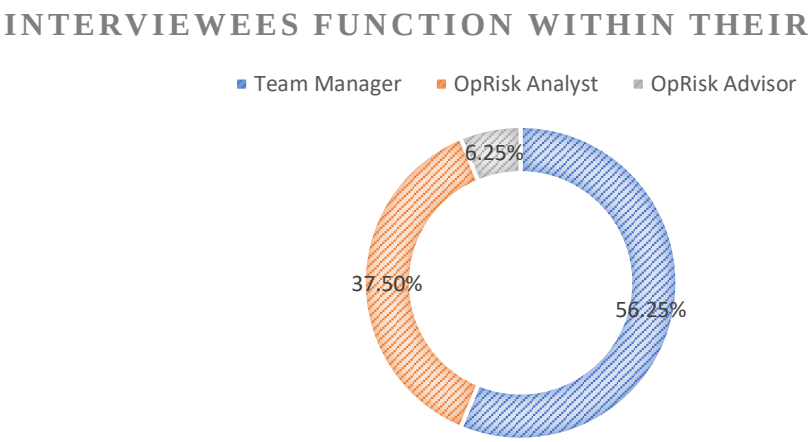


Figure 3.3 - Interviewees functions within their company
Source: Elaborated by the author

Regarding the work experience in OpRisk, as you can see in the Figure 4 below, the interviewees were distributed as follows: 25% having 0 to 4 years of job experience, 31,25% have between 5 to 9 years, 12,5% between 10 to 14 years, 18,75% between 15 to 19 years on OpRisk and lastly, with 20 years or more of experience working in the area are 12,5% of the interviewees.

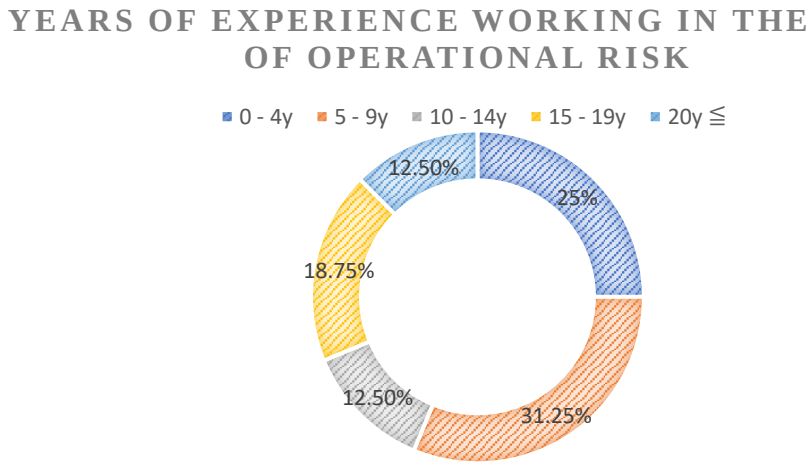


Figure 3.4 - Years of experience from the interviewees working in OpRisk
Source: Elaborated by the author

Chapter 4 - Data Analysis

In this chapter we will proceed to the analysis of the data extracted from the interviews and discussion regarding the implementation of Artificial Intelligence in OpRisk Management

4.1 Success factors of the implementation

The first generic category of this research aimed to explore what are the success factors for the implementation of these technologies in OpRisk. Inside this category we funder explored the pros and cons associated to the use of AI based machines, the most relevant features of these machines, the areas in which the implementation would cause a great impact and finally the outcome, being it the challenges and success factors of the implementation.

Table 4. 1. 1 - Success factors of the implementation considering the pros and cons

Text	Generic Category	Subcategory	Times mentioned	Interviewees
The time spared, costs reductions and the increased efficiency	1.1	1.1.1	10	4, 5, 6, 7, 8, 10, 11, 13, 15, 16
Diminish the OpRisk by diminishing the number of controls done by a human and increase consistency	1.1	1.1.1	7	1, 2, 3, 6, 8, 9, 16
The machine is only as good as the specifications we gave them, we have to regularly question the machine and review it to make sure it is functioning properly	1.1	1.1.1	5	4, 6, 7, 12, 15
Reallocation of human resources from tedious tasks to more added value ones	1.1	1.1.1	4	2, 4, 7, 15
Lack of know-how and lack of human judgement that can mean an increased risk if the robot encounters novelties he was not programmed for	1.1	1.1.1	4	7, 9, 14, 16
It is a hard task to develop the software and put it correctly running	1.1	1.1.1	3	2, 5, 15
Difficult to find a constrain in the implementation of these technologies	1.1	1.1.1	2	1, 3

Source: Elaborated by the author

During the interviews, most of the interviewees recognized that the use of AI based machines in controls will diminish the operational risks that are directly associated with human errors. Table 4.1.1 presents some of the main arguments mentioned by the OpRisk analysts interviewed, regarding the advantages and disadvantages attributed to the use of intelligent systems in the control of OpRisk.

As can be seen, in the view of most of the interviewees the use of this type of systems implies advantages such as time spared in the OpRisk controls, cost reductions in a long run and increased efficiency. Also as mentioned by Chen & Qu (2020) regarding the dimmish of credit risk, it was commonly mentioned the diminish occurrence of Operational risks caused by human error, and consequently an increase in consistency of the analysis of the errors. This will lead us to the topic of human reallocation, that some of the interviewees considered key since it will allow humans to spend more time in more value-added tasks that require professional judgement. This analysis confirm what Aziz & Downling (2018) emphasized, regarding the cost reductions, time sparing and increase in accuracy of the information and also confirms the theory of Shabbir & Anwer (2018) regarding AI machines being able to complement human tasks. However, contrary of what Shabbir & Anwer (2018) predicted, the system is not yet affordable to every organization, being sometimes considered a very expensive initial investment.

When asked about the constraints of this implementation the opinions diverge between the 16 interviewees. The most pointed out constraint was the challenge of giving the machine all the specifications so it can work correctly, also keeping an eye on the robot and review it to make sure it is running properly. Others refer the lack of know-how and the hard task of developing the software. Only 2 interviewees couldn’t find a limitation in this implementation.

Table 4. 1. 2 - Success factors of the implementation considering the most relevant features and areas to implement this ai systems in OpRisk Management

Text	Generic Category	Subcategory	Times mentioned	Interviewees
Improving the motivation of the team by doing less repetitive tasks and doing more value-added tasks	1.1	1.1.2	11	2, 3, 4, 5, 6, 7, 10, 12, 13, 15, 16
Will be more useful in the identification and calculation of risks	1.1	1.1.2	9	3, 4, 7, 8, 9, 10, 11, 13, 16
Can increase the consistency and predictability of the controls performed	1.1	1.1.2	5	1, 6, 8, 10, 11
This system will be very impactful in control management	1.1	1.1.2	4	1, 2, 5, 15
Can be relevant in risk mitigation	1.1	1.1.2	3	6, 12, 14

Source: Elaborated by the author

Regarding the most appropriate areas to implement this AI systems in OpRisk, Milkau & Bott (2018) believed that AI systems had the potential to make decisions and predict solutions. However, the areas of risk identification and risk calculation where the ones most of the interviewees agreed on, as represented in Table 4.1.2 usually with the explanation that these areas are more analytic, and the machines can treat data in an extremely efficient way when compared with human analysts. This means there is still some doubts regarding the capabilities of machine reasoning. Also mentioned is the impact of this implementation in control management functions, which supports the theory of Kolbjørnsrud *et al*. (2016) that these technologies could replace some management functions.

Following the reasoning from the previous table, the reallocation of risk analysts from the more tedious and repetitive tasks will improve the motivation of the teams. Some believe

that this automation will also increase the consistency of the risk controls, and therefore increase the predictability of the risks.

The question of increased defense against spammers, blocking malware attacks, theft of data and financial bases raised by Leo *et al.* (2019) was not mentioned by any of the interviewees, which can mean that this is still an unexplored potential benefit from these technologies.

4.2 Downsides of the implementation

The second generic category of this research intended to reflect the possible downsides or unsuccess factors of the implementation of AI systems in OpRisk controls. In this category we considered the main challenges pointed out during the interviewees associated with the implementation and also tried to comprehend if the interviewees consider the machines a threat to their future and their careers.

Table 4. 2. 1 - Downsides of the implementation considering the main challenges pointed out

Text	Generic Category	Subcategory	Times mentioned	Interviewees
Human Resources capabilities	1.2	1.2.1	8	1, 3, 4, 5, 7, 8, 12, 16
The constant monitorization	1.2	1.2.1	7	2, 4, 5, 6, 7, 9, 13
Losing the added value that the professional judgement can bring to these tasks	1.2	1.2.1	6	5, 7, 8, 9, 10, 15
The biggest challenge is the resistance of human resources to accept change and automation	1.2	1.2.1	6	1, 3, 7, 8, 12, 14
If there is a system with autonomous processes, there will be a reduction on job positions	1.2	1.2.1	6	6, 7, 10, 11, 13, 15
The big investment it is and understand if whether the money spent pays in the future	1.2	1.2.1	5	2, 6, 8, 13, 15

Source: Elaborated by the author

Through the Table 4.2.1 we can perceive that there was no consensus on the main challenges of the implementation of these systems. The opinions diverge from the constant monitorization of the machines, the lack of human resources capabilities to understand the machines and also the resistance of the human resources to accept the change to automation of some functions. Another concern raised where the possibility of losing the value added by the professional judgement and decision making in the controls and, in the worst-case scenario, losing the money invested in this technology.

As Ng (2016) and Shabbir & Anwer (2018) considered, the apprehension of job displacement could be noticed among the interviewees.

One interviewee questioned the human resource capabilities, not due to the lack of understanding the technology, but the physical and psychological impact it would have on the analyst if the routine tasks were automated, as it would mean more complex tasks endorsed to humans every day and this would be a potentially stressful and emotional draining situation.

Table 4. 2. 2 - Downsides of the implementation considering the replacement of human function: is ai a real threat?

Text	Generic Category	Subcategory	Times mentioned	Interviewees
Social and ethical issues can arise from this replacement	1.2	1.2.2	7	1, 6, 7, 9, 11, 13, 15
It would be a complementary work, not a replacement of humans	1.2	1.2.2	6	1, 2, 4, 8, 12, 16
AI will never replace human judgement in OpRisk, it can create new jobs and new tasks if we have time to focus on other things.	1.2	1.2.2	5	1, 2, 4, 7, 16

Source: Elaborated by the author

During the interviewees, when asked about the replacement of humans and human functions by machines, most of the interviewees seemed to understand this replacement as a complementary work for the work of managers and analysts, that would never replace the professional judgement so it could not be considered as a threat, as represented in Table 4.2.2.

In conformity with what Wilson *et al.* (2017) argued, 5 interviewees agreed that these disruptive technologies could create new jobs, with new roles and new skills.

On the other hand, some showed some fears regarding the social and ethical issues that can arise from this replacement of humans for machines, as Wilson et al. (2017) and Haenlein & Kaplan (2019) predicted due to the lack of empathy and depth of the machines. This topic was highly discussed, and it seems it is not considered a problem in OpRisk area, but in all the areas that deal with human resources, where contact with people requires the sensitivity that does not seem possible for a machine. Some fear that the technology of pattern recognition and learning from past experiences may perpetuate existing biases, as feared by Haenlein & Kaplan (2019) when defending the need for regulation.

Some theories we previous mention were not observed in the results of the interviewees. Kolbjørnsrud *et al.* (2016) mentioned her skepticism in the capacity of robots to engage workforce, however there was only one interviewee that mentioned the topic and expressed the complete opposite opinion. Shabbir & Anwer (2018) mentioned the lack of regulation and data protection the primarily issue and Ng (2016) pointed out as a disadvantage the huge amount of data machines require, however there was no concerns raised regarding these thoughts.

Another fear that was not mentioned during the interviews was the one raised by Gonçalves, R.A.H. (2011), when the author questioned the impact robotization will have in the image of the companies in the markets and regarding not being able to fulfil the needs of the companies. Nonetheless it was mentioned several times the lack of ability of machines to replace human judgement, which confirms this idea of the author.

4.3 Main drivers of success or unsuccess

The third generic category of this research meant to find the main drivers of success or unsuccess, what makes the AI systems worth the implementation and what keep companies from acquiring and developing them. For this purpose, this category will approach the perspective of the interviewees that already work with AI based machines in OpRisk to access their opinion, also the perspective of the interviewees that don't work yet with these machines and their projections on it and lastly understand the level of reliability is placed in the machines.

Table 4. 3. 1 - Main drivers of success or unsuccess of the implementation considering the perspective of those who work with ai systems in OpRisk and the overall balance of the implementation

Text	Generic Category	Subcategory	Times mentioned	Interviewees
I already have AI systems automating functions of OpRisk in my company	1.3	1.3.1	7	1, 2, 6, 7, 9, 10, 14
Developing the software was relatively easy for the project itself and its dimension	1.3	1.3.1	6	2, 6, 7, 9, 10, 14
The machine I use performs data gathering functions from tools and reports	1.3	1.3.1	5	2, 6, 7, 10, 14
The overall balance was positive, although it needs constant observation and adaptation	1.3	1.3.1	5	1, 2, 6, 10, 14
The machine we work with have pattern recognition, can learn from previous alerts and have decision-making functions	1.3	1.3.1	4	1, 7, 9, 14
I’m not sure if the balance is positive or negative, I cannot fully trust the machine	1.3	1.3.1	2	7, 9

Source: Elaborated by the author

In the perspective of the interviewees that already work with AI based systems in OpRisk, 6 out of 7 said the development of the software was not a big challenge, some expected worst due to the dimension of the project, some bought a software that was already developed and only had to adapt it to their daily tasks. Only 1 of the interviewees found the software development very hard.

When asked about the functions the machines perform, most of them said to have data gathering from tools and reports, pattern recognition functions, decision-making functions and also a technology that learns from previous alerts. It was also stated the possibility of having more updated information and an adaptive real-time response, has previously said by Milkau & Bott (2018).

From the 7 interviewees, 5 believed the overall balance was positive with the increase efficiency and the more tedious tasks automated, being easier to keep the team motivated. Also mentioned is the decrease in losses that proves what was said by Chandrinos *et al.* (2018) when supporting that these technologies improved the returns of the companies.

Only 2 interviewees were not sure if the balance would be positive or negative yet, both showing low levels of trust and reliability in the AI based machines.

Table 4. 3. 2 - Main drivers of success or unsuccess of the implementation considering the perspective of those who don't work with ai systems in OpRisk

Text	Generic Category	Subcategory	Times mentioned	Interviewees
We don't have AI based systems in the OpRisk department yet	1.3	1.3.2	9	3, 4, 5, 8, 11, 12, 13, 15, 16
The main reason is the lack of resources and having other priority sectors to automate	1.3	1.3.2	8	3, 5, 8, 11, 12, 13, 15, 16
The company is not making any progresses to acquire AI systems for OpRisk at the moment	1.3	1.3.2	6	3, 4, 5, 8, 12, 15
The most important tasks to automate would be the repetitive ones, mainly data gathering related	1.3	1.3.2	6	4, 5, 11, 12, 13, 15
The main struggle would be developing the software and the lack of human judgement in the controls	1.3	1.3.2	5	4, 5, 12, 15, 16

Source: Elaborated by the author

From the perspective of the interviewees that didn't work with AI based systems in OpRisk, 6 out of 9 don't have yet any progresses being made towards the acquisition of these machines and only 3 had projects in their companies to implement this automation within this year.

The reasons suggested for the lack of investment in these systems were very repetitive among the interviewees, most of them pointed out the lack of resources, high initial investment costs and having other priority sectors to automate. When questioned about the sectors that can

have higher priority most of them pointed out the credit risk area as having higher priority in the perspective of the companies.

There was not much disagreement in the important tasks from OpRisk to automate, as most of them choose data gathering functions without reluctance.

Some interviewees showed some apprehension regarding the human resources capabilities, a question raised by Aziz & Downling (2018), and moreover regarding the struggle of developing such a complex software.

Table 4. 3. 3 - Main drivers of success or unsuccess of the implementation considering the level of trust and reliability in the controls performed by ai systems

Text	Generic Category	Subcategory	Times mentioned	Interviewees
I consider the controls performed by an AI based machine as reliable as the controls performed by an analyst	1.3	1.3.3	9	2, 3, 4, 9, 10, 11, 13, 14, 16
The machine is less reliable because only an analyst has the capacity to evaluate and think rationally about the constantly changing OpRisk environment	1.3	1.3.3	5	5, 6, 7, 8, 15
The trust depends on what it measures since it can work perfectly within the parameters, but it wouldn't be able to develop itself and recognize new parameters correctly without human intervention.	1.3	1.3.3	4	5, 8, 10, 14,
The sensibility and the professional judgment will always be important and in some cases can make the difference between an analyst and a machine	1.3	1.3.3	3	12, 13, 15,

Source: Elaborated by the author

As confirmed in the Table 4.3.3 during the interviews the issue of reliability in the machines arose. In this sense, I tried to analyse the level of trust placed in AI based systems when performing functions previously performed by OpRisk analysts.

Although most of the interviewees demonstrated confidence in these systems, there were obviously two opposing positions that divided the respondents. On one side we have the

ones that consider the controls performed by a machine as reliable as the controls once performed by an analyst, and the reasons for this trust are based on being a highly developed technology that showed before their abilities to replace human functions and to upgrade controls performance. This confirms the drivers of success predicted by Gonçalves, R.A.H. (2011) that are mentioned on his investigation. On the other hand, there are the interviewees that cannot rely on the AI based machines as much as they rely on the analysts, claiming that no machine has the capacity to think and evaluate in a rational way that can keep up with all the constant changing OpRisk environment, which means these interviewees don't believe in the ability of AI systems to learn from the previous events and to predict future ones.

Regardless of the reliability expressed, it is noticeable that there is some uncertainty regarding the aptitude of the machine to develop itself and recognize new parameters without human intervention, reinforcing the importance of professional judgement. Contrasting is the noticeable trust in all tasks that involves data treatment, like statistics, a phenomenon anticipated by Leo *et al.* (2019).

It is important to mention that one interviewee seemed completely sceptical about the capabilities of the AI based machines to work in OpRisk, expressing some apprehension regarding the advances of technologies and the possibility of one day being completely replaced by a machine.

Conclusion

Discussion and Findings

Reaching the finishing line in this research, we are now able to take the final conclusions according to the previous results and discussion, extracting the key findings of this investigation.

Starting with the first research question "What are the success factors of implementing Artificial Intelligence in Operational Risk Management?", during the interviews 62,5% of the sample pointed as key success features the cost reductions, the time spared and consequent increased efficiency. From this 62,5%, only 40% were interviewees that already work with AI based systems in OpRisk and 60% had no previous contact with the AI systems in OpRisk, which means that their answers are based on what they expect that the machine would do. This can mean that the machines are living up to the expectations of the analysts since a considerable number of interviewees with experience agreed with this success factors. Another important feature of the implementation of AI based automation, stated by 70% of the sample, is that it motivates the teams giving the fact that analysts have less repetitive and tedious tasks to do.

Still regarding the first research question, 56.3% of the sample believed that the machines would have a greater impact and success in the identification and calculation of risks and not so much in their mitigation. Also, 43,8% of the sample believe that one of the success factors of this implementation is the reduction of OpRisk caused by human errors. From this percentage of the sample, 57% were analysts with AI machines implemented in their daily work and 43% were analysts that already expected this to happen.

It is important to mention that 1 person between the 16 interviewees considered that the software was hard to develop, the remaining interviewees didn't consider it a difficult process bearing in mind the size of the task. So, we can conclude from most of the answers that the software available in the market to implement AI based solutions in OpRisk are a success factor instead of a downside.

Concerning the second research question "Which are the possible down-sides of implementing Artificial Intelligence in Operational Risk Management?" it was clear in the interviews that the most concerning downside is the need for constant monitorization of the machines. This was stated both by analysts with and without experience working with AI based

machines in OpRisk, which means that, even the ones that already work with these technologies, still feel the necessity to always check if the robot is running correctly. The unreliability in these technologies will be further discussed.

The lack of know-how, lack of human judgement and inability to answer to upcoming novelties are the most enumerated constrains of the use of AI machines in OpRisk, mentioned mostly by analysts that already work with these technologies. This reflects the lack of investment from companies both in acquisition of AI technologies itself as well as in qualifying staff to work with this type of technologies. As a result of this, 50% of the sample pointed out the lack of human resources capabilities to deal with the AI machines as a downside and 37,5% of the sample emphasised the resistance of human resources to the implementation of this systems.

An essential possible downside to mention was stated by 44% of the sample that fears the upcoming ethical ad social issues that can arise from the increasing use of this AI based machines. The issues are associated with the possibility of rising unemployment if the machines replace humans in some functions and with the lack of empathy and human judgment. Another 44% of the sample believe that the replacement of humans by machines will never be an issue, considering that the AI machines are only complementary to the tasks made by humans. These analysts even expect to have new jobs and new tasks for humans, since they will have more time to focus on value added tasks and develop other areas that were now forgotten due to the lack of resources. Given the discrepancy of answers, we will not be able to consider the possibility of job reduction a downside, not without considering the possibility of new upcoming tasks and jobs as a success factor.

Lastly, the third research question “Which are the main drivers of success or unsuccess of the application of Artificial Intelligence in Operational Risk Management? Is it worth the application?” aims to understand what are the major barriers and obstacles to achieve the application of AI in OpRisk Management, as well as to find out what are the drivers of success that make the application work. In the end, the objective is to recognize if the application is beneficial or if the overall balance is negative. From the interviews we can extract that one major driver of unsuccess is the inability to develop a machine with the same capabilities of having a professional judgement as a human.

In this RQ3 is important to analyse the view of the people who already work with AI systems in OpRisk in opposition to the view of people who don't. Starting by the interviewees with experience in these technologies, about 43,8% of the total sample, 72% have functions as data gathering from tools and reports automated and 57% said to have pattern recognition, decision-making and machines that learn from previous events. From these interviewees, 85,7% believe the software was easy to develop and 71,4% consider the overall balance positive. The remaining are not sure if the balance will be positive or negative, mostly because they still cannot trust the machine fully.

On the other hand, the interviewees that still don't work with AI systems in OpRisk, 56,2% of the sample, 67% said there were no progresses being made towards the application of AI machines in OpRisk. Also, 89% agreed that the reason for not having the technology yet is both the lack of resources from the companies and the priority that is given to other sectors of the company, such as the credit risk area, when it comes to invest in automation. This proves a major unsuccess factor, while some firms already understood the importance and the impact on the losses that these AI based technologies can have in the mitigation of OpRisks, some companies seem to be dubious on the advantages of investing in the automation of controls and resulting mitigation of OpRisks.

It is also important to notice that, from the 9 interviewees that don't have automated functions yet 6 would see a key advantage in automating the repetitive tasks, pointing the data gathering as an essential task to automate. It is curious to see that 56% of these interviewees think the software development will be a big struggle and a major constraint to implement these machines. As we have seen before, from the answers of the analyst with AI machines implemented in their daily work, the software is actually a driver of success, and so, this shows the lack of information and know-how of these technologies, which can sometimes be the motive of why some companies don't invest.

Finally, in terms of trust and reliability on the machines, the opinions diverge between the elements of the sample. Although we can see in the interviewees a major concern regarding the need of constant monitorization, that lead us to think that there is no trust in the machines, 56% of the total sample acknowledged that the controls performed by AI based machines can be as reliable as the ones performed by an analyst. Some of the interviewees even consider the machines more reliable, as unlike humans, the machines don't get distracted, sick or forget previous specifications. 31% of the sample consider the machines less reliable as a human

analyst due to the lack of rationality and reaction to novelties. From this we can conclude there is still a long way to go when it comes to building trust and being able to truly rely on the machines, as some people are still very sceptical on the technological evolutions around Artificial Intelligence.

Final Considerations

Considering all the content aspects described in this investigation, it seems clear that the biggest obstacle to implementing AI systems in OpRisk Management may be the poor age of the sector, that is still developing itself and the lack of investment in it.

In this investigation, we sought to fill the gap around the literature that covers these two areas, aiming to relate the progress in Artificial Intelligence with its possible application in the control of OpRisk which resulted in the three research objectives mentioned in Table 3.1.1 in the Methodology. The research model of this dissertation emerges from an exploratory and observational basis, being the sample too reduced to generalize the conclusions taken. The data collection implied one-to-one semi-structured interviews, based on the idea of not limiting the interviewees to the script, which allows to achieve diverse types of information that would not be acquired if the interviews were done under a rigid model.

To summarize, the relevant findings to retain from the first research question is that the true success factors of these technologies are the cost reductions and improved efficiency. The reduction of human errors, higher precision in the controls done, and the fact them keeps employees motivated by eliminating the tedious tasks. Also, it was clear that the areas of risk identification and risk calculation are the ones that can have a higher return from the implementation of AI systems in OpRisk. Also, the software solutions available in the market are a success factors, as the majority seems to consider it easy to adapt to their needs.

From the second research question we can conclude that the significant downsides are the need to monitor the machines, the lack of knowledge of these AI technologies and lack of investment in training staff. Also, the lack of human rationality when novelties occur and possible future ethical and social concerns.

The main drivers of unsuccess are the inability of machines to level the professional judgement a human can have, in terms of learning by themselves and making decisions that require rationality. Another driver of unsuccess, probably the most impacting one, is the lack

of investment in OpRisk, as some companies still don't give the area the appropriate attention and acknowledgement for the impact it can have on preventing losses, giving priority to other sectors.

The main drivers of success are the ease and readiness to acquire a software, that although it is an expensive initial investment, is easily adapted to the reality of each firm and so it pays the investment relatively fast. Another driver of success is the trust in the AI machines, if well programmed and running correctly, that can become more accurate than analysts due to the absence of biological and environmental influences.

Limitations

First, it is important to take into consideration that the findings presented in this investigation are limited due to a reduced research in sample size, even though the sample can be considered very heterogeneous in the sector of activity and country of business from the interviewees.

The greatest limitation of this study is the gap in the existing literature that addresses the topic of Artificial Intelligence applied to OpRisk, a previously known limitation that became a target for the development of the topic.

Furthermore, considering that the sample was mainly constituted by interviewees from the banking sector, it is not recommended to reflect the conclusions in the other sectors.

Suggestions for future research

Having in mind the importance to stress the lack of existing literature that study the implications and the applications of AI systems in Operational Risk, my recommendations are all directed to this area of studies.

During the research I realized that, although institutions follow the Basel Committee III recommendations, most of them have a very different way of analyzing and controlling OpRisks, which is an obstacle to a faster adaptation process of the AI based machines software to the daily OpRisk tasks. Following this thought, my suggestion for future studies in this field of studies is trying to find a way to harmonize how institutions from each sector perform their

OpRisk controls, and further develop a software that could be applied to the different institutions in an easier and more harmonize way, without requiring such a time-consuming initial investment.

Another suggestion that may be valuable and convenient is to perform a much deeper and detailed research focused on Portuguese institutions from the banking sector, to further understand how these technologies could have a greater impact in the mitigation and prediction of OpRisks.

Bibliography

Abdul Rahim, N. F., Ahmed, E. R., Sarkawi, M. N., Jaaffar, A. R., & Shamsuddin, J. (2019). Operational risk management and customer complaints: The role of product complexity as a moderator. *Benchmarking*, *26*(8), 2486–2513. https://doi.org/10.1108/BIJ-04-2018-0089

Arian, H., Moghimi, M., Tabatabaei, E., & Zamani, S. (2020). *Encoded Value-at-Risk: A Predictive Machine for Financial Risk Management*. 1–26. http://arxiv.org/abs/2011.06742

Aziz, S., & Dowling, M. M. (2018). AI and Machine Learning for Risk Management. *SSRN Electronic Journal*, 1–18. https://doi.org/10.2139/ssrn.3201337

Bini, S. A. (2018). Artificial Intelligence, Machine Learning, Deep Learning, and Cognitive Computing: What Do These Terms Mean and How Will They Impact Health Care? *Journal of Arthroplasty*, *33*(8), 2358–2361. https://doi.org/10.1016/j.arth.2018.02.067

Boora, K. K., & Kavita. (2018). Implementation of Basel III Norms in Banking Industry: A Review of Empirical Literature. *IUP Journal of Bank Management*, *17*(3), 7–24. http://esc-web.lib.cbs.dk/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=131613195&site=ehost-live

Calo, R. (2017). Artificial Intelligence Policy: A Roadmap. *SSRN Electronic Journal*, 1–28. https://doi.org/10.2139/ssrn.3015350

Chandrinos, S. K., Sakkas, G., & Lagaros, N. D. (2018). AIRMS: A risk management tool using machine learning. *Expert Systems with Applications*, *105*, 34–48. https://doi.org/10.1016/j.eswa.2018.03.044

Cheng, M., & Qu, Y. (2020). Does bank FinTech reduce credit risk? Evidence from China. *Pacific Basin Finance Journal*, *63*(July), 101398. https://doi.org/10.1016/j.pacfin.2020.101398

Diehl, C. A. (2014). Gestão De Riscos Operacionais: Um Estudo Bibliográfico Sobre Ferramentas De Auxílio. *Gestão De Riscos Operacionais: Um Estudo Bibliográfico Sobre Ferramentas De Auxílio*, *19*(3), 41–58. https://doi.org/10.12979/10408

Drucker, P. (2014). Banco de Portugal - Risco Operacional. *Newsletter Biblioteca BdP*, *nº 1*, 1–6.

Fadun, O., & Oye, D. (2020). Finance & Banking Studies Impacts of Operational Risk Management on Financial Performance: A Case of Commercial Banks in Nigeria. *Fadun and Oye / International Journal of Finance & Banking Studies*, *9*(1), 2020. www.ssbfnet.com/ojshttps://doi.org/10.20525/ijfbs.v9i1.634

Giannone, F. (2018). Operational Risk Measurement: A Literature Review. In P. Leone, P. Porretta, & M. Vellella (Eds.), *Measuring and Managing Operational Risk: An Integrated Approach* (pp. 95–143). Springer International Publishing. https://doi.org/10.1007/978-3-319-69410-8_3

Gonçalves, R. A. H. (2011). *Sistemas de Informação para Gestão de Risco Operacional em Instituições Financeiras*.

Haenlein, M., & Kaplan, A. (2019). A brief history of artificial intelligence: On the past, present, and future of artificial intelligence. *California Management Review*, *61*(4), 5–14. https://doi.org/10.1177/0008125619864925

Jakhar, D., & Kaur, I. (2019). Artificial intelligence, machine learning and deep learning: definitions and differences. *Clinical and Experimental Dermatology*, *45*(1), 131–132. https://doi.org/10.1111/ced.14029

Kolbjørnsrud, V., Amico, R., & J. Thomas, R. (2016). How Artificial Intelligence will Redefine Management. *Biometrika*, *94*(2), 487–495. https://doi.org/10.1093/biomet/asm033

Leo, M., Sharma, S., & Maddulety, K. (2019). Machine learning in banking risk management: A literature review. *Risks*, *7*(1). https://doi.org/10.3390/risks7010029

Luburić, R. (2017). Strengthening the Three Lines of Defence in Terms of More Efficient Operational Risk Management in Central Banks. *Journal of Central Banking Theory and Practice*, *6*(1), 29–53. https://doi.org/10.1515/jcbtp-2017-0003

Milkau, U., & Bott, J. (2018). *Active Management of Operational Risk in the Regimes of the " Unknown ": What Can Machine Learning or Heuristics Deliver ? i*. https://doi.org/10.3390/risks6020041

Moro, S., Cortez, P., & Rita, P. (2015). *Business intelligence in banking : A literature analysis from 2002 to 2013 using text mining and latent Dirichlet allocation*. *42*, 1314–1324. https://doi.org/10.1016/j.eswa.2014.09.024

Nadikattu, R. R. (2016). *The Emerging Role of Artificial Intelligence in Modern Society*. *4*(4), 906–911. http://www.netsci.org/Science/Special/feature06.html

Nadikattu, R. R. (2018). Artificial intelligence in IT. *Ubiquity*, *64*(August), 1–12. https://doi.org/10.1145/3266135

Nadikattu, R. R. (2019). New Ways in Artificial Intelligence. *SSRN Electronic Journal*, *67*(12), 89–94. https://doi.org/10.2139/ssrn.3629063

Ng, A. (2016). What Artificial Intelligence Can and Can't Do Right Now. *Hbr*, 9–12.

Peters, G. W., Shevchenko, P. v., Hassani, B., & Chapelle, A. (2016). Should the advanced measurement approach be replaced with the standardized measurement approach for operational risk? *Journal of Operational Risk*, *11*(3), 1–49. https://doi.org/10.21314/JOP.2016.177

Shabbir, J., & Anwer, T. (2018). *Artificial Intelligence and its Role in Near Future*. *14*(8), 1–11. http://arxiv.org/abs/1804.01396

Smith, A. (2020). *Artificial Intelligence : In Banking A Mini-Review*.

Vőneki, Z. T. (2018). *Operational risk after the crisis*. 315–328.

Weeserik, B. P., & Spruit, M. (2018). Improving Operational Risk Management using Business Performance Management technologies. *Sustainability (Switzerland)*, *10*(3). https://doi.org/10.3390/su10030640

Wilson, H. J., Daugherty, P. R., & Morini-Bianzino, N. (2017). The jobs that artificial intelligence will create. *MIT Sloan Management Review*, *58*(4), 14–16.

Annexes

A – Interview Script

1) **For statistical matters, in which country do you work?**
2) **To what sector of activity does the company where you work belong to?**
3) **For how long do you work in operational risk?**
4) **What kind of functions do you perform?**
5) **In your workplace, have you incorporated any type of AI based software to automate functions that were previously delegated to employees?**

   IF YES

   i. **Which type of automation have you implemented? What are the functions that are automated?** (RQ1: What are the success factors of implementing Artificial Intelligence in Operational Risk Management?)

   ii. **Was it a difficult process to develop the software? (**RQ1: What are the success factors of implementing Artificial Intelligence in Operational Risk Management?)

   iii. **Can you please state, from your experience, the pros and cons of implementing AI systems in operational risk controls?** (RQ1: What are the success factors of implementing Artificial Intelligence in Operational Risk Management?)

   iv. **With all the pros and cons in mind, do you consider that this automation had a positive or negative overall balance? And why?** (RQ3: Which are the main drivers of success or unsuccess of the application of Artificial Intelligence in Operational Risk Management? Is it worth the application?)

v. **After the implementation completed, please name the main challenge and the main success factor.** (RQ3: Which are the main drivers of success or unsuccess of the application of Artificial Intelligence in Operational Risk Management? Is it worth the application?)

IF NO

i. **What are the main reasons that led you to not have automated functions yet?** (RQ2: Which are the possible down-sides of implementing Artificial Intelligence in Operational Risk Management?)

ii. **Do you know if progresses are being made towards the application of AI systems in the process of operational risk management?** (RQ1: What are the success factors of implementing Artificial Intelligence in Operational Risk Management?)

iii. **From your experience, which are the priority functions to automate?** (RQ1 & RQ2: What are the success factors of implementing Artificial Intelligence in Operational Risk Management? Which are the possible down-sides of implementing Artificial Intelligence in Operational Risk Management?)

iv. **Considering that you don't have automated functions yet in your daily job, which do you think would be the pros and cons of implementing AI systems in OpRisk controls?** (RQ1 & RQ2: What are the success factors of implementing Artificial Intelligence in Operational Risk Management? Which are the possible down-sides of implementing Artificial Intelligence in Operational Risk Management?)

6) **In your opinion, what are the most relevant features in these AI based systems?** (RQ3: Which are the main drivers of success or unsuccess of the application of Artificial Intelligence in Operational Risk Management? Is it worth the application?)

7) **What is your impression in using AI technologies to replace humans in certain functions? Do you fear future social or ethical issues?** (RQ1 & RQ2: What are the success factors of implementing Artificial Intelligence in Operational Risk Management? Which are the possible down-sides of implementing Artificial Intelligence in Operational Risk Management?)
8) **Do you consider the automation of OpRisk controls as reliable as the operational risk controls performed by a risk analyst? Why?** (RQ3: Which are the main drivers of success or unsuccess of the application of Artificial Intelligence in Operational Risk Management? Is it worth the application?)
9) **In what areas of OpRisk management do you think AI can have the most relevant impact?** (RQ3: Which are the main drivers of success or unsuccess of the application of Artificial Intelligence in Operational Risk Management? Is it worth the application?)
10) **What are the main challenges of applying AI in OpRisk management?** (RQ3: Which are the main drivers of success or unsuccess of the application of Artificial Intelligence in Operational Risk Management? Is it worth the application?)