DOCTORAL THESIS

CREATING AN ENTERPRISE RISK MANAGEMENT (ERM) MODEL FOR IDENTIFYING AND EVALUATING THE OPERATIONAL RISKS FOR A TELECOMMUNICATIONS COMPANY. A CASE STUDY

Author:

José Ruiz-Canela López

Supervisor:

Francisco Javier Forcadell Martínez, PhD

Social and Legal Sciences Doctoral Program

Line of research: Management

International Doctoral School

2021

TESIS DOCTORAL

CONSTRUCCIÓN DE UN MODELO DE GESTIÓN DE RIESGOS CORPORATIVOS (ERM) PARA LA IDENTIFICACIÓN Y EVALUACIÓN DE LOS RIESGOS OPERACIONALES DE UN EMPRESA DE TELECOMUNICACIONES. APLICACIÓN A UN CASO PRÁCTICO

Autor:

José Ruiz-Canela López

Director:

Dr. Francisco Javier Forcadell Martínez

Programa de Doctorado en Ciencias Sociales y Jurídicas

Línea de investigación: Empresa

Escuela Internacional de Doctorado

2021

DEDICATION

In memory of my Father

"All roads have their risks, but the most dangerous may be to stand still for fear of facing them" (Aaron Wildavsky[1], 1930–1993).

"Todos los caminos tienen sus riesgos, pero lo más peligroso puede ser quedarse parado por miedo a afrontarlos" (Aarón Wildavsky[2], 1930–1993).

[1]Aaron Wildavsky was an American political scientist known for his pioneering work in public policy, government budgeting and risk management.

[2] Aaron Wildavsky fue un politólogo estadounidense conocido por su trabajo pionero en políticas públicas, presupuestos gubernamentales y gestión de riesgos.

CONTENTS

FIGURES[3]

[3] When the source is not included in any figure, it should be understood that it is "author's own elaboration".

TABLES[4]

[4] When the source is not included in any table, it should be understood that it is "author's own elaboration".

ABSTRACT

Operational risk is defined as the potential losses resulting from events caused by inadequate or failed processes, people, equipment, and systems or from external events. One of the most important challenges for the management of the company is to improve its results through its operational risk identification and evaluation. Most Enterprise Risk Management (ERM) scholarship has roots in the financial sector and there is a lack of studies in other industries such as telecommunications. This research study proposes an innovative operational risk identification and evaluation model, based on a case study approach for a telecommunications company (TELCO), the main pillars of which are the operational risk identification frameworks for events, risk factors and risk effects, as well as the development of an operational risk assessment methodology, on the basis of an operational risk self-assessment process and method. The operational risk self-assessment process evaluates operational risks through a quantitative analysis of estimates the inputs of which are the economic impact and the probability of occurrence of events. The operational risk self-assessment method is the “engine” for calculating the economic risk impact, applying actuarial techniques, which allow estimation of unexpected and expected loss distributions in TELCO. The results of the analyzed business units in the field work for the case study were compared with standardized ratings (acceptable, manageable, critical, or catastrophic), and contrasted against the company’s managers, proving that the operational risk identification and evaluation model is a reliable and useful management tool for the business and its stakeholders, and leading to more research in other sectors where operational risk management is key for the company success.

RESUMEN

El riesgo operacional se define como las pérdidas potenciales resultantes de eventos causados por la inadecuación o fallos en los procesos, las personas, los equipos y sistemas o por factores externos. Uno de los retos más importantes para la gestión de la empresa es mejorar sus resultados mediante la identificación y evaluación del riesgo operacional. La mayor parte de los estudios sobre la gestión del riesgo empresarial (ERM) tiene su origen en el sector financiero y faltan estudios en otros sectores, como el de las telecomunicaciones. Este estudio de investigación propone un modelo innovador de identificación y evaluación de riesgos operacionales, basado en un enfoque de estudio del caso de una empresa de telecomunicaciones (TELCO), cuyos pilares principales son los modelos de identificación del riesgo operacional para los eventos, los factores de riesgo y los efectos del riesgo, así como el desarrollo de una metodología de evaluación del riesgo operacional, sobre la base de un proceso y un método de autoevaluación del riesgo operacional. El proceso de autoevaluación del riesgo operacional evalúa los riesgos operacionales a través de un análisis cuantitativo de estimaciones cuyas entradas son el impacto económico y la probabilidad de ocurrencia de los eventos. El método de autoevaluación del riesgo operacional es el "motor" para calcular el impacto económico del riesgo, aplicando técnicas actuariales, que permiten estimar las distribuciones de pérdidas inesperadas y esperadas en TELCO. Los resultados de las unidades de negocio analizadas en el trabajo de campo para el caso de estudio fueron comparados con calificaciones estandarizadas (aceptable, asumible, crítico o catastrófico), y contrastados con los gestores de la empresa, demostrando que el modelo de identificación y evaluación del riesgo operacional es una herramienta de gestión fiable y útil para la empresa y sus grupos de interés, y dando lugar a más investigaciones en otros sectores donde la gestión del riesgo operacional es clave para el éxito de la empresa.

ACKNOWLEDGEMENTS

To my family, friends, and all my loved ones, always encouraging and supporting me, who know how much enthusiasm and effort I have put into the development of this new milestone in my academic development, just trying to contributing a drop of water in the immensity of the ocean of scientific knowledge. I would especially like to thank my friend Fran, my thesis director and my mentor who has made it possible for this work to come to fruition.

1 INTRODUCTION

The motivation to write a thesis about risk management comes from the idea that the concept of risk touches on the most profound aspects of human psychology, mathematics, history and firms' management. In general, the risk literature is vast, and each day's headlines bring many new items of interest, which made us selective in choosing the approach with most impact: the discipline of risk management for improving the business results within a company to which the author of this thesis dedicated almost 30 years. Bernstein (1998), in his description of the remarkable story of risk, introduces a question: "what is it that distinguishes the thousands of years of history from what we think of as modern times?", arguing that "the answer goes way beyond the progress of science, technology, capitalism and democracy" (p. 1). This is good "food for thought" in the sense that a common aspect for any decision that we make, as individuals, groups of people or organizations, is that we all face uncertainty. Risk is everywhere and derives directly from unpredictability, both in daily life activities and in relevant business decision-making processes. Mastery of risk makes it possible to define the boundary between modern times and the past, inspired by the ancient beliefs about the whims of the gods. The ability to foresee what may happen in the future and to choose among alternatives is always a challenge for contemporary societies and companies. The consequences of recent events in the world, such as terrorism, financial crisis, extreme weather or the current global pandemic which started as COVID-19, have brought risk into higher profile. These extreme risks that are facing societies and enterprises coexist with mundane risks as mentioned before (Hopkin, 2010). However, the consequences of events on a global scale and in people's personal lives could include the creation of new and valuable opportunities, such as an appreciation for what we have as individuals and society and for what we want to keep for the future. Useful in this regard are: (i) the implementation of the basic principle of total quality of prevention, "prevention versus control" (Ruiz-Canela López, 2004) (p. 87) in any activity or decision we make; (ii) contingency and business continuity plans in case something goes wrong; (iii) dedication to more investment for research, development and innovation; and most importantly, (iii) awareness of lessons learned from past experiences and critical events. Following this, Rubino (2018) explains that risk and uncertainty bring negative outcomes and positive opportunities.

The definition of risk in the Spanish language dictionary (*Real Academia Española* [RAE], 2014) refers in some way to what providence holds, contingency or proximity of danger; while for the Oxford English Dictionary the concept of risk is understood as a possibility of danger, loss, injury or other adverse consequences (OED, 2010). In both

basic definitions, risk is used to signify negative consequences; however, taking risks is the essence of business management and daily life as they can also result in a positive outcome, being a third possibility that risk is related to uncertainty of outcome. The concept of risk has a variety of origins. A basic definition is provided by the Institute of Risk Management (Hopkin, 2010) as a "the combination of the probability of an event and its consequence. Consequences can range from positive to negative" (p. 12), while OED (2010) provides a basic definition of risk management in only negative terms of attempting to identify and manage threats that could bring down the organization. Further definitions of risk and risk management are explored in this study to fulfil its objectives by creating a prior common language within the organization, which is a key success factor for deploying risk management.

Another relevant context to consider is that the modern risk approach comes from a string of large public organizational and governmental failures and financial scandals over the past 20+ years (Citigroup and Enron, which will be described later, are just examples of these situations) that have focused the attention of regulators, investors and customers on the way directors are managing risk. Also, Abkowitz (2008) provides a series of descriptions of real operational disasters such as the World Trade Center attacks on September 11th, 2001 or the Sumatra-Andaman tsunami on December 26th, 2004, as well as some success stories and lessons learned.

A common aspect of organizations is that they face uncertainty in their strategic and operational decisions, and risk management provides a framework for organizations to deal with uncertainty. The modern practice of risk management is a systematic approach, based on comprehensive standards that help in improving business resilience, increase predictability and fulfil the business organization's fundamental purpose through value creation for stakeholders. These are usually represented by customers, shareowners, employees, shareholders, suppliers and by the social impact they produce (Krause and Tse, 2016). Two main industry-sanctioned models – COSO-ERM frameworks (Committee of Sponsoring Organizations of the Treadway Commission [COSO], 2004; COSO, 2017), and ISO 31000 standards (International Organization for Standardization [ISO] 31000, 2009; ISO 31000, 2018) – help in managing various risk types that organizations face (Karaca and Senol, 2017). Beals *et al.* (2015) explain that Enterprise Risk Management (ERM) facilitates the awareness of risk factors which helps management in decision-making. The focus of COSO-ERM and ISO 31000 frameworks and standards is deploying a risk management process for the business, enabling the adoption of best practices with the stakeholders' support. Among all the stakeholders, it

is relevant to stress the importance of ERM in shaping shareholder value both in developed and developing economies. In their study of ERM program implementation for specific firms, Hoyt and Liebenberg (2011; 2015) found a positive correlation between firm value and ERM deployment. McShane *et al.* (2011) also found a positive association between Standard and Poor's ERM quality rating and company value within the insurance industry. In financial organizations, risk management has always played a central role based on shareholder value concepts (Dickinson, 2001). Additionally, for non-financial firms, a positive relationship was found between ERM and their values, even over the financial crisis period from 2001 to 2011 (Anton, 2018). Bertinetti *et al.* (2013) found a positive statistical relation between ERM implementation and firm value for financial and non-financial industries. Manab and Ghazali (2013) concluded in their research that each type of organization, whether profit or non-profit, provides value for its stakeholders. They also analyze that risk management practices affect shareholder value on certain aspects of risk management variables; for non-financial companies, less regulated than financial companies, almost all variables have an impact on shareholder value. The findings of Lechner and Gatzert (2018) show that size, international diversification, and the industry sector (banking, insurance, and energy) positively impact the implementation of an ERM framework, leading to shareholder value creation. Furthermore, Gatzert and Martin (2015) conducted a comparative assessment of empirical evidence study regarding the determinants of ERM and its value once implemented, which showed a relevant positive impact on corporate value and performance. Additionally, the research of Altuntas *et al.* (2020) reviews various studies to confirm the positive relationship between ERM adoption and value creation for firms, pointing out that their performance increases after ERM program implementation. Finally, it is important to consider that risk management is a sensitive subject, particularly with respect to external stakeholders, which should not be overlooked due to the difficulty of sharing critical information that could be misinterpreted or compromising (De Lima, 2004).

As will be discussed in the theoretical foundation, risk identification and risk evaluation are the most important steps of the risk management process. In order to implement this risk management philosophy within the company, events need to be identified and evaluated, stating that the published ERM frameworks and standards have some limitations, such as the lack of risk identification and evaluation techniques to be implemented in specific sectors (e.g. telecommunications). Accordingly, one of the most important challenges for the management of the company is to improve its results through its operational risk identification, evaluation, and management, operational risks

being the most basic and common events for any business unit in an organization (Callahan and Soileau, 2017). Operational risk is defined as the potential losses resulting from events caused by inadequate or failed processes, people, equipment, and systems or from external events (Basel Committee on Banking Supervision [BCBS], 2006). Although this definition and the frameworks and techniques based on it seems to be relevant and applicable only to the financial sector, the conclusions of the discussion panel on risk management held in the University of Georgia (2005), support the idea that the approaches focused on an integrated risk management model were a significant strategic interest for most operational functions in any type of industry.

In summary, one of the most important challenges for the management of the company is to improve its results through its operational risk identification and evaluation, which is the core objective of this research by creating and applying an innovative model to help managers of firms, researchers and practitioners in gaining insight and practical implementation of the risk management discipline within the telecommunications sector. The scientific contribution developed in this research, known as knowledge transferability or technology transfer (Matkin, 1990; Pererva *et al.*, 2012), aims to help organizations in achieving the challenge mentioned in enhancing their operational and financial performance.

The thesis is organized as follows. After including an introduction to the thesis, the research objectives (main purpose and research questions), and the scientific contribution, in the theoretical foundation we present and explain the fundamentals of risk management, a literature review on previous studies on operational risk identification and evaluation, a current context of risks in the telecommunications sector, some theoretical conclusions and the study propositions. Next, we present the empirical study, which includes the research design and the development of research objectives, i.e., the model and results, in identifying and evaluating the operational risks for a telecommunications company. Finally, in the conclusions, we include the main findings, contributions and practical implications for researchers and practitioners, future lines of research, limitations and managerial implications.

Furthermore, at the time of development of this research, the coronavirus COVID-19 pandemic did not exist. Otherwise, this risk would have been one of the biggest materialized events in terms of severity. This catastrophic event would have been discussed under the “Black Swan” theory (Taleb, 2010) which refers to unexpected events of major impact, considered extreme outliers with a low or regular likelihood of

occurrence, and even considered classified as a global risk due to its overall impact in all the areas of TELCO (the case study company), i.e., included with huge impact in operational and non-operational (mainly business and financial) categories of risk. Although this special situation is not within the scope of this study, due to the time period of the research elaboration, mention should be made of the impact that COVID-19 has been having on risks, the global coronavirus pandemic (GCP), not only on health consequences, social distancing and lockdown measures and their profound economic impacts, but also recognizing that COVID-19 is the most significant event for businesses since the global financial crisis of 2008. Unfortunately, it is expected to cause a deeper recession, higher rates of unemployment and bigger increases in public debt. Businesses and their risk profiles have been significantly affected by GCP. References to the COVID-19 coronavirus pandemic have been included in specific sections of this study, it being unavoidable to mention this crisis when discussing risks.

Note 1: Please note that the main contents of the published article "How Can Enterprise Risk Management Help in Evaluating the Operational Risks for a Telecommunications Company?" (Ruiz-Canela López, 2021) have been incorporated into this thesis (see Appendix B).

Note 2: For ethical considerations for all the participants in the empirical study of this research, and for confidentiality issues, TELCO Group and TELCO company have intentionally not been referred to by their real names (corporate names).

1.1 Research objectives

There are opportunities for generating risk management models for value creation within telecommunications companies, despite the facts that: (i) several enterprise risk management studies question the validity of these models arguing that they may turn out to be theoretical and too general approaches to have a successful practical application in the companies (Beasley *et al*., 2005; Fraser and Simkins, 2016; Lundqvist, 2014); and (ii) this limitation is bigger in respect of the challenge of identifying and evaluating operational risks for a large telecommunications company, where there is a lack of contrasted studies versus all the assessment (identification and evaluation) models implemented in the financial sector (Bromiley *et al*., 2015; Kozarevic and Besic, 2015; Sehrawat, 2019; Yesuf, 2017). Thus, the primary **purpose** of this study is to create and apply an operational risk identification and evaluation model for a company in the telecommunications sector.

Based on this main purpose, the associated research questions are:

- **Research question I**: How can a telecommunications company identify its operational risks?
- **Research question II**: How can a telecommunications company evaluate its operational risks?

The propositions[5] of this research, based on the study's main purpose and research questions, and once the theoretical foundation supporting the empirical study has been developed, are stated in sub-section 2.5. They refer to the creation and application of an operational risk identification and evaluation model for a company in the telecommunications sector based on: (i) the theoretical conclusions (sub-section 2.4); and (ii) the formulation of a lean, useful and practical (easy to implement) risk management process framework containing two basic steps: risk identification and risk evaluation (sub-section 2.1.3).

1.2 Scientific contribution

Enterprise Risk Management scholarship has roots in the finance/risk management and insurance (RMI) discipline. In fact, the most studied tested experiences about the use of operational risk identification and evaluation methods belong to financial and insurance disciplines (Chernobai *et al.*, 2007; McShane, 2018), mainly in the banking sector, through models such as Basel II (BCBS, 2006; 2009). In the telecommunications sector, there is a lack of research in creating risk management models. In fact, while McShane *et al.* (2011) rely on the financial services industry to analyze good practices in risk identification and evaluation techniques, Monda and Giorgino (2013) indicate the limitations of finding similar identification and quantitative evaluation methods for other industries, such as telecommunications. The literature of previous studies on operational risk identification and evaluation reviewed in this study evidences this restriction.

Furthermore, though various scientific works show that there is a general consensus that the growth in popularity of COSO-ERM frameworks and ISO 31000 standards has resulted from a response to pressure on organizations to holistically manage risk, nevertheless, other studies (Lundqvist, 2004) question the validity of these frameworks and standards arguing that they may turn out to be too theoretical and general to have a successful practical implementation in firms. Even with the COSO-ERM prominent

[5] Section 2.5 explains the difference between the terms propositions and hypotheses, given the nature and objectives of this research.

framework and the globally accepted risk management standard ISO 31000, organizational contexts make a one-size-fits-all process of implementing ERM unfeasible, especially in the telecommunications sector due to lack of research mentioned. Also, the standard ISO Guide 73 (2009), a well-developed risk management vocabulary reference for reducing miscommunication within the company, is not enough to create a common language for an efficient and practical development of ERM.

This research study seeks to address the limitations above. It has the objective of creating, describing and applying an operational risk identification and evaluation model for a company in the telecommunications sector. Based on a case study approach, the main pillars of the model for companies in the telecommunications sector are: (i) the events, risk factors and risk effects identification frameworks (OpRIF); and (ii) the development of a risk assessment methodology (OpRAM), supported by an operational risk self-assessment (OpRSA) process and method. The OpRSA process evaluates operational risks through a quantitative analysis of estimates, the inputs of which are the economic impact and the probability of occurrence of events. The OpRSA method is the "engine" for calculating the impact of economic risk, applying actuarial techniques which estimate unexpected loss and expected loss distributions in TELCO. The results of the business units analyzed were compared with standardized ratings (acceptable, manageable, critical, or catastrophic), and contrasted against the company's managers. This proves that the OpRSA framework is a reliable and useful management tool for the business, and leads to more research in other sectors where operational risk management is key for the company's success. The companies implementing risk management models based on ERM for risk identification and evaluation achieve high financial results and receive the best evaluations from the market (Florio and Leoni, 2017).

Furthermore, the scientific contribution of this study is foreseen considering the abovementioned research objectives and four characteristics aimed at achieving them: (i) technology transfer; (ii) relevance; (iii) originality; and (iv) non-triviality. Regarding the research objectives, the scientific contribution will be successful if the operational risk identification and evaluation model created is robust, useful and practical. Also, it is necessary that the analysis of the results can provide a transferable, relevant, original and non-trivial knowledge about the model and its practical application and contributions as described in section 4 of this study. A brief summary of the scientific contribution objectives includes the following: (i) creation of an innovative operational risk model based on universally-accepted ERM frameworks, where there is a lack of literature and

experiences for the telecommunications sector; (ii) real application of the model to a complex telecommunications company, where frameworks, processes and methods can be extrapolated to other firms and industries in different sectors, for enhancing their business results, and therefore, stakeholders' satisfaction; (iii) development of key managerial contributions in terms of operational risk identification and evaluation, setting up of a business "tool" as a best practice for helping firms' managers in their decision-making processes; and (iv) deployment of practical implications for company's management and for researchers and practitioners, contributing to the business environment and the academic community in consolidating theoretical concepts and a practical approach for the ERM discipline.

This study can be understood as **technology transfer** (knowledge transferability) research. Transferability is established by providing researchers and scholars with evidence that the study's findings could be applicable to other contexts, situations, times, and populations (Guba and Lincoln, 1985). Basically, the way transferability is applied is by giving a range of experiences and results on which the reader can build understanding to decide whether the research is applicable to practice in a specific situation. In summary, results transferability (where *transferens* is its Latin root) is a dissemination process of scientific information, based on translating theoretical models into professional or academic practice. This research aims to provide knowledge on an operational risk management model, tools and practical application based on results transferability to researchers, scholars, academics, and business managers and specialists, who may need to develop their experiences in the field of knowledge of risk management. As mentioned in section 1 (introduction), technology transfer is the most up-to-date and accurate term for this characteristic. Matkin (1990) examines the relationship between university research and the growing importance of technology transfer through discussing and comparing the history of this concept in four major American research universities: University of California (Berkeley), MIT (Massachusetts Institute of Technology), Stanford University and Penn State University (Pennsylvania State University).

In the context of the complexity of the business in the present society, as well as considering the risk approach challenge as further described throughout this research, the **relevant** interest of this study is supported by the fact that firms need practical risk management models, customized to their respective sectors, that allow them to respond to operational, legal and regulatory requirements, and to satisfy their stakeholders in terms of an efficient business management to achieve excellent results. The creation,

description and application of an operational risk identification and evaluation model for a telecommunications company, which may be useful for its decision-making processes, would contribute to become a best practice for the firms of the telecommunications sector. It would also be beneficial to any other business where the lessons learned from this research can be implemented. Thus, the stakeholders would benefit from a quality risk management framework, not only for the financial sector, where we can find vast literature, but also for a critical sector such as telecommunications, in order to identify and evaluate operational risks, which are critical for achieving and enhancing the firms' goals. Therefore, internal and external customers, shareholders, shareowners, suppliers, and administrations and society in general, by applying this innovative model and knowledge, would be granted with control and management frameworks for treating their operational risks in their products and services.

As described by Soriano (2008), the concept of **originality** refers not only to the authorship of the work (authenticity), but also to the idea that the research contributes something really new (novelty), i.e. being able to accomplish any type of new knowledge about a little known or hardly explored subject (Coromina *et al.*, 2002). The identification and assessment through operational risk models represents an innovative and original line of research as, based on the literature review, there is scarce bibliographical evidence nor practical implementation of these models in the telecommunications sector. At present, operational risk identification and evaluation models which allow practical and useful implementation in non-financial sectors are scarce in the literature.

Furthermore, the subject and objectives of this thesis can be identified as scientific research, specific, viable and with a reasonable difficulty (realistic scope). The design and application of an operational risk management model in such an unexplored sector (telecommunications) in this field of knowledge (risk management) is **not a trivial** task, moreover considering that the field work is a tedious process due to the expected sensitive nature of the information to be gathered and the potential difficult access to the interviewees (managers). Furthermore, the non-triviality is evident through the development of concepts which the managers of TELCO case study, *a priori*, are not familiar with or they are not used to them in their decision making processes, such as risk appetite, severity, likelihood, loss distributions, among others; as well as getting their buy-in in a new model that could not have been implemented without management involvement and understanding of new approaches and terminology.

2 THEORETICAL FOUNDATION

This section reviews the fundamentals of risk management, previous studies on operational risks and offers an updated view of the main operational and business risks identified by renowned and prestigious sources of information. From this review, we derive some propositions that constitute the basic reference for the empirical study.

2.1 Fundamentals of risk management

In recent decades and even currently, many entrepreneurs tend to avoid talking about the problems associated with the risks in their firms. Urquijo (1993) states that this silence is because they understand that a risk is understood as a measure of failure (it is not usually seen as a business opportunity or a lesson learned, as will be discussed). Talking about a danger may be a weakness and the company could not fulfil one critical mission to promote confidence among the stakeholders. However, most enterprises currently look upon risk management as a basic need for daily and efficient management. Risk management is a systematic process that includes identifying and evaluating a company's risks and implementing action plans in accordance with the undesirable events that may materialize. In fact, accepting specific risk would allow firms to make relevant profit through preventive actions more than reactive initiatives to mitigate potential losses. In this case, the firm would benefit from an efficient risk management strategy and favorable market conditions.

Currently, the management of many firms' (mainly from the financial sector) have developed processes for identifying and evaluating operational risks based on the Basel II Accord (BCBS, 2006), while other corporations are still planning how to implement these integrated operational risk management models.

The practices that will be described have been evolving into new approaches based on COSO frameworks and ISO 31000 standards, which consider the basic objectives and values of the company, developing mechanisms that need to be customized or built to identify, measure, monitor and review the risk strategy continuously and efficiently.

COSO, the most relevant commission for internal control and risk management, is the Committee of Sponsoring Organizations (COSO), a voluntary private-sector organization dedicated to improving the quality of financial reporting through business ethics, effective internal control and corporate governance. COSO was originally formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting, an initiative

referred to as the Treadway Commission. The sponsoring organizations are the American Institute of Certified Public Accountants (AICPA), The Institute of Internal Auditors (IIA), Financial Executives International (FEI), Institute of Management Accountants (IMA) and American Accounting Association (AAA). This Commission (COSO) is dedicated to providing thought through the development of frameworks and guidance on ERM, internal control and fraud deterrence. It also studied the causal factors that can lead to fraudulent financial reporting and developed recommendations for public companies and their independent auditors, for the U.S. Securities and Exchange Commission (SEC) and other regulators, and educational institutions.

The International Organization for Standardization (ISO) was founded on 23 February 1947 in London with headquarters in Geneva, and is an independent, non-governmental and international standard-setting body composed of representatives from more than 165 members countries with their standards organizations. The founders are the International Federation of the National Standardizing Associations (ISA) and the United Nations Standards Coordinating Committee (UNSCC). This organization develops and publishes worldwide technical, industrial, and commercial standards. Standards are the distilled wisdom of people with expertise in their subject matter and who know the needs of the organizations they represent: manufacturers, sellers, buyers, customers, trade associations, users or regulators. For example, quality management standards to help work more efficiently and reduce product failures; environmental management standards to help reduce environmental impacts, reduce waste and be more sustainable; health and safety standards to help reduce accidents in the workplace; energy management standards to help cut energy consumption; food safety standards to help prevent food from being contaminated; and/or IT security standards to help keep sensitive information secure.

The International Electrotechnical Commission (IEC) was founded on June 26 1906 in London with headquarters in Geneva, is an international standards organization that prepares and publishes international standards for all electrical, electronic and related technologies, collectively known as "electrotechnology". IEC International Standards are essential for quality and risk management; they help researchers understand the value of innovation and allow manufacturers to produce products of consistent quality and performance. There is a close collaboration between ISO and IEC.

The purpose of this section is to review the basic concepts of the risk management discipline, understanding of which is essential to fulfil the main objective of this research:

the creation, description and application of an operational risk identification and evaluation model for a telecommunications company.

2.1.1 Risk, risk management and business opportunities

2.1.1.1 Evolution of the risk management discipline

It is important to analyze risk management evolution to better understand the terminology of this discipline and the points of view for value creation through this discipline. The risk management area of knowledge emerged significantly in the mid-1970s, as an evolution of insurance management concepts and activities (Barlow, 1993). These activities are usually associated with natural disasters, fires, thefts and employee illness levels. New activities included in the new way of managing risks are related to product reliability, employment practices, environmental degradation, accounting, compliance and exchange rate fluctuations, among other events.

As described by Espiñeira *et al.* (2008), during the eighties and since the early 1990s, this global approach to risk management became increasingly more intensive due to higher sensibility of firms in respect of country risks and the impact of large fluctuations in the financial markets. For this reason, as will be explained, it was necessary to put in place additional control mechanisms for financial institutions.

In the years prior to 2000, RIMS (the Risk Insurance and Management Society), one of the main professional organizations for risk management, began to assess areas for new development of the operational risk management discipline, including environmental risks (mainly pollution and waste), as well as business ethics risks. Furthermore, this organization began to consider other risk types associated with financial aspects such as exchange and interest rate fluctuations and guarantees in e-commerce through the internet. RIMS (2009) also describes the financial crises in 2008.

According to Espiñeira *et al.* (2008), the various risk categories started to be configurated from a broader view than the traditional hedge (cover), as they are organized around the macroeconomic and microeconomic spheres. From the macro point of view, the categories were related to potential natural disasters and industrial and financial practices before the crisis. At the microeconomic level, the risks were classified in line with the processes and company activities that should lead to excellent business results with expected losses under control. These controls, unfortunately, were not able to avoid fatalities such as the Windsor fire in Madrid, or the financial scandals of emblematic

corporations such as Barings Bank, Natwest Bank, Enron, Allied Irish Bank, Citygroup (Worldcom), Tyco, Parmalat, and Lehman Brothers, where the stakeholders and/or customers were defrauded. Concerning these relevant cases of financial and operational losses, some examples of important cases of operational losses are included as follows, for illustrative purposes: (i) 1995: Barings Bank. Losses: $1,300 MM. Nick Leeson, a trader at the British bank Barings, spent two years accumulating undeclared losses and trading derivatives contracts from the bank's Singapore branch. The bank failed; (ii) 1996: Barings Bank. Losses: $2,600 MM. An employee of the entity traded copper contracts in the London metals market that accumulated undisclosed losses over three years; (iii) 1997: Natwest Bank. Losses: $127 MM. Kyriacos Papouis, a financial trader in the over-the-counter options market, used incorrect volatilities to value the products, overvaluing the contracts; (iv) 2001: Enron. Losses: $40,000 MM. The company utilized special purpose vehicles to hide its toxic assets and large amounts of debt from investors and creditors; its shareholders lost $40,000 million in the four years leading up to its bankruptcy, and its employees lost billions in pension benefits. (v) 2002: Allied Irish Bank. Losses: $691 MM. A trader in the foreign exchange market concealed three years of losses in operations on the yen/dollar exchange rate; (vi) 2002: Citigroup (Worldcom case). Losses: $2,650 MM. The president of WorldCom corporation, Bernard Ebbers, and former CFO Scott Sullivan committed a series of accounting frauds that led to the company's bankruptcy. The banking group Citigroup had to reach an out-of-court settlement with shareholders who were paid $2,650 million in exchange for withdrawing their class action lawsuit because the bank was involved in the fraud by recommending WorldCom securities even though it knew details of the company's weak financial situation; (vii) 2002: Tyco. Losses: $600 MM. Theft in Tyco by former company CEO and Chairman Dennis Kozlowski and former corporate Chief Financial Officer Mark Swartz of as much as $600 million from the firm; (viii) 2003: Parmalat. Losses: $4,500 MM. Two former Parmalat chief financial officers, Fausto Tonna and Luciano Del Soldato, and two executives at the Italian affiliate of the global auditing group, Grant Thornton, committed fraud when it was revealed that a $4,500 million bank account held by a Cayman Islands unit did not exist. Management sought bankruptcy protection, and prosecutors launched a criminal fraud probe; (ix) 2005: Windsor case. Losses: Not officially estimated to date. The fire at the Windsor building in Madrid resulted in the loss of profits of countless businesses and bank branches that were within the security perimeter. The assets contained in many of the offices in the building have not yet been declared or valued; and (x) 2008: Lehman Brothers. Losses: $3,900+MM. Under the leadership of Richard Severin Fuld, as Chairman of Lehman Brothers, the company became heavily involved in the mortgage market, owning the subprime mortgage seller BNC Mortgage.

As Lehman had held onto, or could not sell, so many risky low-rated mortgages, the subprime mortgage crash affected the bank badly and, in the first half of 2008, it lost 73% of its value. That created the financial crisis that led to the Great Recession. This financial crisis of 2008 altered so many lives: millions of people lost their homes, their jobs and their savings; and though the crisis grew out of big banks' handling of mortgage-backed securities, no Wall Street executive went to jail for it.

The evolution of risk management discipline can be understood following the concept of Traditional Risk Management (TRM), and develops the history of risk management in three corporate stages (also called silos): insurance management, financial risk management, and internal control and auditing. The concept of insurance management, developed before the mid-1950s, involved purchasing insurance to transfer hazard risks such as property damage, product liability and worker safety. Based on these insurance practices, Kloman (1992) studied the concept of risk management emphasizing the importance of applying a process to proactively manage risk rather than just financing after the loss occurs. The financial risk management stage development started in the mid-1970s and was based on the growth in the financial derivatives industry, its associated hedge financial risks and other financial instruments, including: insurance practices for currency, interest rate, commodity price and credit risk. A third corporate risk management stage arose after financial scandals in the late 1980s and early 1990s. New commissions were created to redefine the mission of the internal control function to include risk management and corporate governance roles for internal auditors (Spira and Page, 2003; Huber and Rothstein, 2013). Regulators, rating agencies, firms and academics reacted to corporate scandals and business failures over the past 20+ years developing focus on risk management. In response to this third silo, in the mid-1990s, an ERM approach was proposed to integrate management of all risks that organizations face, integrating corporate governance and strategic view (Simkins and Ramirez, 2008). Currently, supporting practices, particularly in the financial sectors and listed companies in the stock market, mainly the SEC (the U.S. Securities and Exchange Commission), include the Sarbanes-Oxley Law (Sarbanes-Oxley Act [SOX/SOA], 2002) and Basel II principles (BCBS, 2006). These regulations apply assessment methods for adequate risk management. SOX is facilitating large corporations in implementing risk management as a preventive and control function. The financial scandals in North American companies as a result of accounting and corporate governance non-compliance, were pretended to be mitigated through SOX implementation of the strictest requirements of control over financial information.

As shown in Figure 2.1, the evolution of risk management has been developed from a traditional vision based on reactive management (e.g. insurance activities) to a current view characterized by the proactive management concept of ERM. Attributes of risk management as a support function, the exclusive concept of risk as a danger, communication of risk only through a loss or negative news for the company or the cost of operational risk not understood and only captured for financial consideration, have evolved to become a function dedicated to the active management of business risks in advance, a proactive process that integrates risk management into the company's strategy for opportunity generation, where it highlights the stakeholder pressure to understand the range of risks the company is facing as well as acquiring the knowledge of the underlying risks which allows capital allocation to be managed more appropriately, thereby increasing value for stakeholders. Figure 2.1 also emphasizes the idea that a company which faces no risk is losing business opportunities; these ones belong to the positive "side of the coin" in the risk management discipline. All these concepts, such as the definition of risk, risk management, risk standards and frameworks, control self-assessment techniques, risk maps, as well as the various laws and regulations (e.g. SOX), are formalized in the following sections. In any case, whatever the proposed recommendations (models, frameworks, standards), risk management will always involve a significant amount of uncertainty (Lupton, 1999).

Figure 2.1. Evolution of Risk Management

2.1.1.2 Approaches to defining risk

In any field of life, the revolutionary idea that delimits the frontier between the modern era and the past is mastery of the discipline of risks (Bernstein, 1998). Throughout the history of mankind, there has been an attempt to understand the nature of risks, how to measure them, the consequences of their materialization, as well as actions to face and coexist with them. Through risk management, achievements in different fields of knowledge and behaviors have been unveiled, including the human passion for gambling and betting, economic growth, improvement in the quality of life and technological progress.

From a macroeconomic point of view, in the context of the events that have taken place in the global financial system over the last few decades, companies have been showing increasing interest in risk management, hence its importance. A proactive approach to risk management allows companies to achieve areas of opportunity in at least three dimensions. In the efficiency of their operations thanks to early identification and actions to contain the costs of events that may disrupt operations, more effective operational processes and projects consider the risks involved and the possibilities available in business operations, and in the effectiveness of the strategy involved in the company's decision-making processes (Hopkin, 2010).

Concerning the concepts of uncertainty and value creation, it is well known that companies operate in changing and highly competitive environments, characterized by factors associated with business globalization, the increased use of information technology, organizational restructuring and process reengineering, as well as constant market evolution. All this facilitates a natural level of uncertainty. This is due to the inability to pinpoint and accurately determine the occurrence of potential events and their impacts or consequences. Organizations face a wide variety of risks that can impact their operations. These risks can have a negative impact (pure risks or hazard risks in Anglo-Saxon literature, which comes from the word *zahr*, which is dice in Arabic), a positive impact (opportunities) or create uncertainty about their effect (control or project risks).

One way of understanding risk management is through pure risks that are solely related to negative consequences for the company. The management of these risks concerns aspects such as health and safety in the workplace, fire prevention, damage to property, as well as impacts due to the production of defective products. Other risks included in this typology are those related to infrastructure and information systems failures, theft

and internal and external fraud. These are all examples of risks that we will classify as operational, and which are very much present in firms in the telecommunications sector.

In understanding risks as opportunities, it is relevant to consider the relationship between these risks and the rewards associated with managing them. Any business operation involves a certain amount of risk that companies assume in the hope that this challenge will turn into an opportunity, and this is what gives meaning to the statement that without risk, except in special cases, opportunities that lead to the achievement of business objectives cannot be activated. This idea of correlating the management of a risk with the reward it can bring can be extrapolated even for pure risks (by decreasing the probability of adverse consequences or their negative impact or both) and for risks associated with projects (improving the probability that they will be implemented on time, within budget and according to the specifications and expected quality of the projects).

Another aspect to consider in understanding risk management is that organizations can adopt different attitudes towards risk. Depending on the nature of each business activity and its state of maturity, organizations can be risk-averse or risk-aggressive/risk-prone. One of the major contributions of risk management is to ensure that strategic decisions that may be considered high-risk are actually made with all available information. This does not prevent the occurrence of the so-called "Black Swans" (Taleb, 2010) or disastrous events when the probability of their occurrence is low or very low.

According to COSO (2004), value is created, preserved or driven by management decisions, from strategy setting to the day-to-day operations of the company. In this sense, decisions inherently bring with them risks and opportunities, which require management to study and analyze information about the internal and external environment, allocate resources and recalibrate the company’s business activities in order to adjust to the circumstances. Companies create value when shareholders recognize benefits on the increase in equity. For government entities, value is created when the citizens of the particular society or community recognize that they receive a quality service at an acceptable or reasonable cost. Shareholders of non-profit organizations create value when they recognize that they receive socially valued benefits. Integrated enterprise risk management enables and empowers management to create and communicate value to shareholders.

To judge the extent to which current methods of risk management are oriented towards

analyzing whether they represent a benefit or a threat to the company, it would be necessary to know the history of their evolution. Many of today's ideas for sophisticated risk management and business decision-making have their origins in gaming and their subsequent modeling through game theory. In fact, the Ancient Greek word *eikos*, which meant plausible or probable, had the same meaning as the modern concept of probability: that which is expected with some degree of certainty. Socrates defined *eikos* in terms of probability of being true. The word risk derives from the old Italian (*risicare*, *riscio* or *rischio*) meaning to dare. The classical Arabic word *rizq* means what providence holds in store (what is yet to come). In this sense, risk for a company could be a business opportunity rather than a concept associated with uncertain and negative fate. The actions that the company dares to take, and which will depend on the degree of freedom they have to make decisions, is the essence of the concept of risk and opportunities for any business. Regarding the basic concepts of risk, the modern term risk has its origins in the Hindu-Arabic numerical system that reached the Western world eight hundred years ago, in the years following 1654, in the flourishing Renaissance. It was at this time that the first more rigorous studies on risks were carried out, most of them by mathematicians such as Pascal and Fermat, who were the precursors of probability theory, the starting point for numerous studies on risk management. Almost two hundred years earlier, in the 15th century, the monk Luca Paccioli, the inventor of double accounting, and his disciple Leonardo da Vinci were the inspiration for these wise men of the time who drew on a game of chance between two players in which one player has an advantage over the other (Bernstein, 1998).

According to the definitions already provided on the term risk by the RAE (2014) and the OED (2010), the word risk is used to indicate negative consequences of some event or occurrence. However, taking risks can also result in positive outcomes or uncertainty. Moreover, from a business point of view, the word risk is not limited to the insurance business; RAE (2014) also includes the concepts of credit risk, interest risk, market risk, reinvestment risk, specific risk, operational risk, country risk, systemic risk and sovereign risk, among the many types of risks that exist.

From a more practical point of view, and in order to understand the definitions reviewed below, a distinction can be made between speculative or pure risks (those that include the possibility of loss or gain) and operational risks (those that exclusively refer to the possibility of loss). In the first case it is important to identify the causes of the events, while in the second case the analysis focuses on the identification of effects and impacts. Additionally, it is useful to distinguish between the concept of an inherent risk (the risk to

an organization in the absence of any action plans that might improve the risk's gross likelihood or gross impact) and a residual risk (the remaining risk's net likelihood and net impact after taking actions and implementing controls) (COSO, 2004).

BSI 31100 standard (British Standards Institution [BSI] 31000, 2007) defines risk in a simple way by referring to something that might happen and its effect(s) on the achievement of objectives. Those risks relate to the potential for both negative impacts (threats) and positive impacts (opportunities). In terms of the ISO risk is understood as the combination of the probability of occurrence and the impact of a given event, considering that the possible consequences of the event can be both positive and negative. Specifically, the concept of risk refers to the effect of the lack of certainty about the objectives, with the possibility of experiencing a deviation from expectations in both directions. ISO Guide 73 (2009) associated with ISO 31000 (2018) standard defines risk as "the effect of uncertainty on objectives. An effect is a deviation from the expected – positive and or negative. Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process)" (p. 1). This definition indicates that a risk can be described as an event, a change in circumstances, a consequence or a combination of all these concepts and how these events can affect the achievement of certain objectives.

According to the Institute of Internal Auditor ([IIA], 2004; 2009) and the *Instituto de Auditores Internos* ([IAI], 2006), risk is defined in terms of the possibility that an event will occur (likelihood) which will impact (result or effect of an event) an organization's achievement of objectives. In this way, risk is measured in terms of impact and probability of occurrence.

It is essential to formulate a definition of risk to understand the approach to risk management through conceptual models and operational processes. Thus, the European Foundation for Quality Management ([EFQM], 2005) refers to risk as a "combination of the probability of an event and its consequence. This definition encapsulates both up and downside risks; consequences can be good or bad. It also states that risks contain an event, as opposed to causes of events" (p. 8). In practice, it is often helpful if other types or discrete occurrences, such as circumstances, actions and situations are also considered (Hopkin, 2002). The revised version of this EFQM model (EFQM, 2019) includes the basic sub-criterion "Driving Performance & Manage Risk" (p. 2). This definition, aligned with ISO Guide 73 (2009), describes that the

consequence can be positive or negative for the company. In addition, the concept of event is identified, distinguishing it from the cause of the event, which helps to differentiate the different identification models part of the development of this research. This definition allows risk to be understood as the potential damage that may arise from a present process or future event, or as the probability of an adverse event, impact or consequence occurring. In this way, it can also be understood as the measure of the possibility and magnitude of adverse impacts, being the consequence of the hazard, and is related to the frequency with which the event occurs. Risk combines the probability of a negative event occurring with how much damage such an event would cause. In other words, risk is the possibility that a hazard could materialize. For a risk to materialize, the event must occur.

Furthermore, and from a social point of view, the term risk (Kates, 1985; Renn, 2008) denotes the probability that an undesired state of reality (adverse effects) may occur as a result of natural events or human activities. This definition implies that causal relationships may occur between events, so that the consequences, in certain situations, may be altered, either by modifying the initial activity or by mitigating the impacts that may occur. This concept is relevant in the identification of events, risk factors and risk effects. In a broader sense, the impacts derived from the materialization of risks can be positive (opportunities) or negative (threats) for the company.

In business practice, there is a tendency to model the losses from a possible materialization of risk using the variables frequency or probability of occurrence and severity or impact (Panjer, 2006). This point of view is supported by experience that demonstrates the usefulness of defining risk as a measure of potential economic loss or injury in terms of the probability of occurrence of an undesired event together with the magnitude of the consequences. For example, given the risk of a possible crime of physical robbery in a bank, action could be taken through the frequency variable or likelihood (which would be reduced by implementing dissuasive measures such as greater police presence or security teams) or the impact variable or severity (by limiting the amount of cash on hand).

In addition, the concept of risk is related to the possibility of something happening that impacts on certain objectives, and should be measured in terms of consequences or impacts and their frequency (Klugman *et al.*, 2004). These concepts help to understand the need for a management model that allows risk management, given that risks are uncertain future events, which may influence the achievement of the objectives of

organizations, including their operations. Such is the importance of defining objectives in the context of risk management that, as Fraser and Simkins (2008) argue, without objectives, theoretically, there should be no risk; that is, if a threatened objective cannot be identified, the risk may not be worth paying much attention to, or alternatively, the objective should be reformulated. Furthermore, although risks can be related to other aspects of the organization (such as its key processes and the expectations of its shareholders), the standard approach (Hopkin, 2010) is to relate the risks of the company to its corporate objectives. Thus, definitions of risk that consider in their formulation the impact (negative, positive or uncertainty) on the company's objectives are useful.

There are other useful definitions of risk, which reinforce the basic variables for risk measurement. The Orange Book (2004) defines risk as "uncertainty of outcome, whether positive opportunity or negative threat, of actions and events. The risk has to be assessed in respect of the combination of the likelihood of something happening, and the impact which arises if it does actually happen" (p. 9). Hopkin (2010) defines risk in terms of the process which aims to help organizations understand, evaluate and act on all their risks with a view to increasing the probability of success and reducing the likelihood of failure as well as "event with the ability to impact (inhibit, enhance or cause doubt about) the mission, strategy, projects, routine operations, objectives, core processes, key dependencies and / or the delivery of stakeholder expectations" (p. 12). Regarding project management, Project Management Body of Knowledge ([PMBOK], 2013) describes risk as "an uncertain event or condition, that if it occurs, it has a positive or negative effect on a project's objective, such as scope, schedule, cost and quality" (p. 310). Regarding the concept of risk, COSO (2004) defines risk in terms of the possibility that an event will occur and adversely affect the achievement of objectives of the company. This definition has been completed in COSO (2017) to reflect the evolution of this concept from the point of view of an integrated risk management or ERM (Enterprise Risk Management), where it is no longer considered relevant only to prevent the erosion of enterprise value or to minimize risk to an acceptable level. Therefore, COSO (2017) defines risk in terms of the possibility that events will occur and affect the achievement of strategy and business objectives. COSO (2017) approach highlights that risk relates to the potential events, often considered in terms of severity, where an event is an occurrence or a set of occurrences, uncertainty is the state of not knowing how or if potential events may manifest, and severity is a measurement of considerations such as likelihood and impact of events or the time it takes to recover from events. This is the definition that we have adopted, for its simplicity and clarity, for the development of this research. In this sense, the events that could occur in the business environment could

have a negative impact, a positive impact or both types at the same time. Those with a negative impact represent risks that may impede value creation or erode existing value. Events with a positive impact can offset negative impacts or represent opportunities which derive from the possibility of an event occurring that positively affects the achievement of objectives, helping to create or preserve value. The management should channel the opportunities that arise, so that they revert to the strategy. In addition, the process of defining objectives should formulate plans to take advantage of them. Figure 2.2, in its definitions, summarizes this formulation of risk versus business opportunities, as well as the COSO II and COSO IV risk definitions.

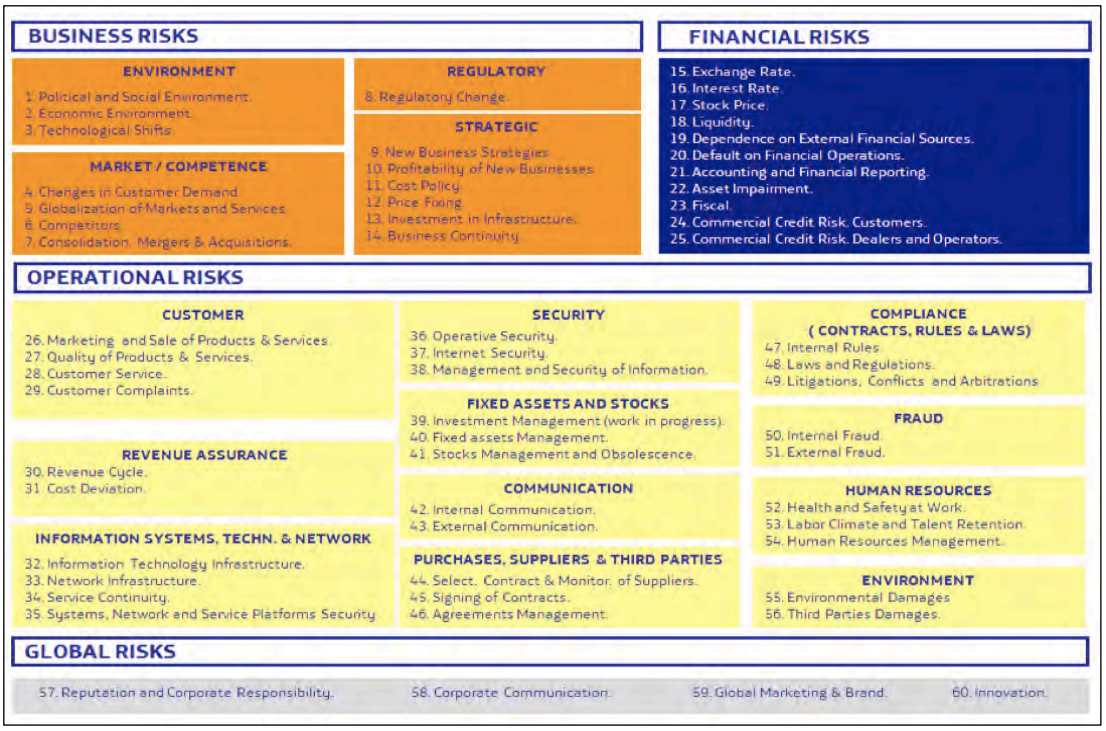
Figure 2.2. COSO Risk Definitions

Finally, having reviewed different definitions of the concept of risk, we illustrate below some categories for organizing the risks of a company. One of them, basic and commonly used, classifies them as strategic, operational, financial and hazard (D'Arcy and Brogan, 2001; Elliot, 2013). Even though ERM scholarship has roots in the finance and insurance disciplines, research has mainly, even solely, focused on financial and hazard risks, as they are easily identifiable and quantifiable types of risk, where operational and strategic risks are more difficult to be analyzed.

Furthermore, for the concepts which support the ERM holistic approach for operational risks, such as risk appetite, corporate governance and breaking down risk management silos, there is a lack of tested experiences and tools in their management, compared to financial risks where the rules have been studied for decades (Bharathy and McShane, 2014). In any case, it is widely known that ERM is oriented towards the comprehensive management of all the company's risks. Within this general idea of ERM, numerous risk

classifications have been put forward. One of these classifications distinguishes between business, financial, operational, and global risk, as shown in Figure 2.3, another illustration of a complete risk classification.

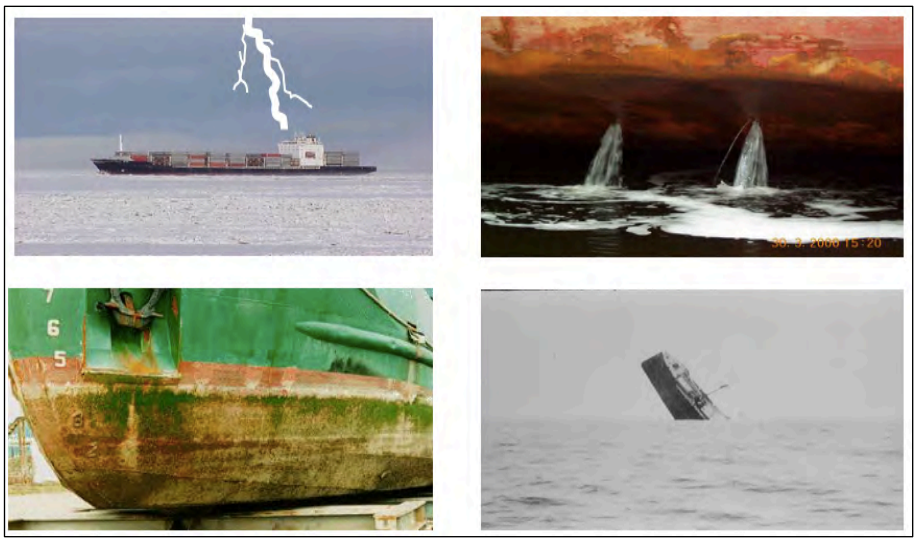
Figure 2.3. Risk Classification. Illustration



Upon initiating the implementation of an operational risk identification and evaluation model, one of the main tasks is to agree upon the definition of operational risk in order to limit and determine the model's scope. Based on Basel II (BCBS, 2006), a practical definition of operational risk would read in terms of potential losses of value or profit arising from events caused by the inadequacy or failures of processes, people, equipment and systems or from external events. This definition includes compliance risk, but excludes strategic and regulatory risk. Operational losses include economic, non-economic and reputational effects. Each industry should consider revising this definition in order to adapt it to its own characteristics and include all its usual operational events.

Figure 2.4 depicts an illustration of operational risk to show the importance of defining risk, the consequent risk classification as well as the required actions. Let us consider the different examples based on the impact variable, which can occur on a vessel (boat).

Figure 2.4. Risk Classification by Impacts on a Boat. Illustration



In the first situation, we have the boat struck by lightning. Damage occurs very quickly with immediate and potentially significant loss and insufficient response time, requiring preventive action. In the second example, leaks are detected on the boat hull, and damage occurs more slowly. In this case there is a gradual and increasing loss with sufficient response time where supervision actions are required. The third situation shows how the boat hull is deteriorated significantly and damage occurs in a spaced and continuous manner, i.e. there is an increasing and potentially significant loss with relatively long response time for repairing it and where professionals need to know the event to implement contingency plans. Finally, we have a shipwreck, which is a catastrophic event with immediate loss at a final phase and remote chance of recovery, in many cases due to negligent action or the effect of a “Black Swan” (Taleb, 2010).

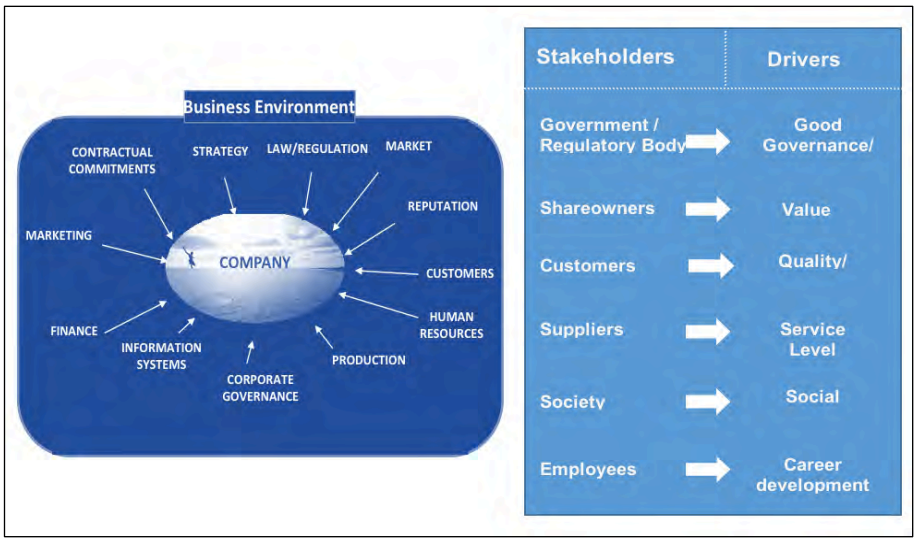
2.1.1.3 Development of risk management

Before providing a formal and useful definition of risk management and the concept of ERM, it is necessary to consider that the shift between TRM (Traditional Risk Management) and ERM approaches came from new definitions and descriptions that have been evolving from the traditional “risk management” term to an “umbrella” and innovative concept based on aspects such as: emerging paradigm (Barton *et al.*, 2002; Beasley *et al.*, 2005; Selim and McNamee, 1999; Silvestri *et al.*, 2011); a truly holistic, integrated, forward looking and process-oriented approach (Deloach, 2000); a systematic and integrated approach (Dickinson, 2001); a strategic business discipline (RIMS, 2011); an evolution of risk management (Fraser *et al.*, 2008); an evolving discipline (Mikes and Kaplan, 2013); and a process approach (COSO, 2004).

Concerning business and industry, we live in a world where managers often ask themselves various questions: how the market is influenced by new entrants and competitors, how are the potential changes within a company for the adoption of a new laws or regulation, or what are the potential risks of daily operations that might jeopardize the achievement of business objectives, among many others. All this has to do with the risk factors. In the business environment, a risk factor is considered any fact or circumstance that may increase the probability of leading to a potential damage in a company.

Because we live in a period of political, economic, technological, competitive and health turbulence, among others, the uncertainties in the business world lead to the following external risk factors: (i) political-regulatory environment (e.g. compliance with laws, corporate governance, new imposed regulation, regulatory bodies for the business and political events); (ii) economic and financial environment (e.g. country macroeconomic stability, capital flow, monetary and fiscal policies, exchange and interest rates, economic-financial devaluations, price of oil and inflation); (iii) competitive environment (globalization of markets, mergers and acquisitions, customer demands, sector-industrial conditions, operational-technical capacity); and (iv) technological, environment and health (e.g. digital revolution, technological tendencies, new business models, climate change, natural events, health crises). On the other hand, and considering that change is constant within organizations, these are the main internal risk factors: (i) business model changes (e.g. new business strategies, launch of commercial offers, infrastructure investments, price fixing, strategic operations with partners); (ii) financial-accounting management (e.g. credit risks, accounts of the organization and agreements management with financing institutions, revenue cycles, cash-billing management, control of fixed assets, fiscal compliance); (iii) compliance with laws and regulations (e.g. internal policies and standards, internal and external fraud, transparent processes before the law, information security); and (iv) adaptation to customers' needs (e.g. quality of products and services, customer care complaints, marketing chain). As shown in Figure 2.5, and to face the various risk factors that influence a company, risk management becomes a need for firms justified by two main reasons: (i) the existence of a great diversity of current and potential risks in business activities due to the growing complexity of the company environment; and (ii) the requirement to have management models considering stakeholders' expectations or drivers, and corporate governance good practices.

Figure 2.5. Risk Management Need and Stakeholders' Drivers



In this context, EFQM (2005) identifies as key benefits of risk management with: (i) the value added and safeguarded organization through seizing opportunities, avoiding threats and, therefore, reducing uncertainty, for tangible assets and intangible assets as goodwill and reputation; (ii) the compliance with laws and regulations; and (iii) the improved stakeholder confidence and assurance through the alignment of risk exposure and organization's objectives, mission and values. Based on this, EFQM (2005) considers risk management as a systematic approach to identify, assess, manage and monitor risks, to support the achievement of the mission and statement to satisfy/exceed the expectations of key stakeholders and organizational objectives. A simpler definition is provided by ISO Guide 72 (2009) as "coordinated activities to direct and control an organization with regard to risk" (p. 2). Also, IRM (2002) provided the following and clear definition of risk management in terms of the process whereby organizations methodologically address the risks attached to their activities to achieve sustained benefit within each activity and across the portfolio of all activities.

Based on the abovementioned definitions and benefits, we can propose the following main risk management objectives to be fulfilled: (i) identifying events that may impact on the achievement of business goals; (ii) performing risk evaluation and risk treatment; (iii) integrating risk management into the company strategy, internal control and daily operations for decision-making processes; and (iv) building a risk profile and portfolio of the organization's challenges and opportunities for value creation and profitability. In summary, we consider that the definition of risk management that best fits the ideas presented and the objectives of this research is the one proposed by COSO (2004): "Enterprise Risk Management is a process, affected by an entity's board of directors,

management and other personnel, applied to strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives" (p. 16). Risk appetite is the amount of risk, on a broad level, an organization is willing to accept in pursuit of value (COSO, 2017); in fact, it is the total value of the resources that the organization is willing to put at risk, i.e. what the organization is willing to achieve. This concept is different from risk capacity (level of risk the organization considers itself capable of absorbing based on business viability, i.e. what the organization is able to achieve) or risk tolerance (reasonable variability of risk acceptance based on the organization's risk capacity and risk appetite, i.e. what the organization is ready to achieve).

The COSO (2004) definition of risk management is adopted in this research study, as we considered it to be the one which deals with risks and opportunities enhancing value creation for the stakeholders and reflecting fundamental characteristics of ERM such as: (i) an ongoing process flowing through an entity; (ii) implemented by people at every level of an organization; (iii) applied in strategy setting; (iv) applied across the enterprise, at every level with a portfolio view of risk; (v) designed to identify and evaluate potential events, to manage risk within the organization's risk appetite; (vi) able to provide reasonable assurance to management and board of directors; and (vii) geared to achievement of the company objectives. COSO (2017) simplifies the definition of ERM in terms of the culture, capabilities, and practices, integrated with strategy and execution, that organizations rely on to manage risk in creating, preserving, and realizing value, which is completely aligned with the COSO (2014) definition. Furthermore, Bromiley *et al.* (2015) also provide various definitions and descriptions of ERM found in the literature review from 1996 to 2011, that COSO-ERM framework definitions have completely overtaken. Finally, regarding the project management discipline, the Project Management Body of Knowledge (PMBOK, 2008) stated that risk management was a necessary organizational tool to control and monitor projects and to potentially achieve goals and objectives. PMBOK (2020) defines the risk management process as the systematic process of identifying, analyzing, and responding to project risks.

2.1.2 Risk management frameworks and standards

In order to deploy any risk management model, we need to consider the international standards for supporting it, defining the key elements, activities and processes for their design and implementation. Based on the scope of the system to be developed, we can classify the standards as: (i) general, which consider all types of risk regardless of their

nature (e.g. COSO, ISO 31000, ISO 31010, ISO Guide 73, BSI 31100); and (ii) specific, associated with the types of risk (e.g. COBIT – The Control Objectives for Information and Related Technology – and ITIL – Information Technology Infrastructure Library – for technological risks, Basel and Solvency for financial risks, ISO 14000 for environmental risks, ISO 19600 for compliance risks, ISO 37001 for anti-bribery management systems, ISO 9001 for quality management systems).

As we can see, there are several standards and frameworks to guide companies in implementing ERM. Some of them are mentioned by Lundqvist (2014) and Perera (2019): COSO, ISO 31000, the joint Australia/New Zealand 4360-2004 standards, the Turnbull guidance, the Casualty Actuarial Society framework, the International Association of Insurance Supervisors framework, COBIT, Standards and Poor's ERM framework, and Basel II. The most frequently mentioned, and particularly used for risk identification and evaluation in this study, are COSO's ERM integrated frameworks (COSO 2004 or COSO II; COSO 2017 or COSO IV) and ISO 31000 standards (ISO 31000 2009; ISO 31000 2018). For this reason, this section is mainly focused on ISO 31000 standards and COSO frameworks, which are the well-known and best documented practices for risk management. After their analysis in the context of the case study of this research, we decided to use the COSO framework, in particular COSO (2004), as the most suitable approach. In fact, the reference model used for operational risk identification and operational risk evaluation in this study is COSO II for three reasons:

- it includes all the key elements for building operational risk identification frameworks and an operational risk assessment methodology (process orientation, effected by people of an organization and strategically related to a top management approach, designed to manage potential events within its risk appetite-value of resources that the organization is willing to put at risk, and goal oriented). This is evident in the COSO (2004) framework's definition of ERM
- the prior existence of a COSO-based internal control framework for assessing TELCO's risk map which was already in place and known in the organization and which was intended to be developed and improved to allow economic quantification of risks. TELCO's managers felt comfortable with this approach in terms of methods and "language" (vocabulary)
- COSO II provides a practical approach for risk identification and evaluation. Moeller (2007) is a good reference for a clear understanding of the COSO (2004) framework.

COSO (2017), which is the latest version of this framework, puts more emphasis on how ERM links strategy, risk, and performance, but it does not add to COSO II any relevant aspect for risk identification and evaluation purposes. Nevertheless, it is also analyzed as it includes strategic, performance and cultural insights needed to understand the impact of the implementation of an ERM model.

We also concluded that ISO 31000 implementation for risk management, in any of its versions, implies an in-depth understanding of all the concepts detailed in the standard by the managers involved in a risk identification evaluation process and method (e.g., risk analysis, risk evaluation, risk assessment, risk treatment, and the interrelation among them). Leitch (2010) considers that the terminology included in ISO 31000 is too ambiguous and does not offer much guidance to managers to the point that it leads to illogical decisions and is impossible to comply with; for example, the definition of risk provided by ISO 31000 is unclear and not enough “mathematically” based. Also, for these reasons ISO 31000 was not considered a practical approach for the objectives of this study. In summary, ISO 31000 creates unnecessary challenges for those who use language and approaches unique to their area of work but different from this standard (Purdy, 2010). Furthermore, as studied by Lalonde and Boiral (2012), in managing risks through ISO 31000, managers must question their own assumptions in the implementation of such a standard, and consider the specificities of their organizational environment while being vigilant in its monitoring, a hard task for people who are not subject matter experts on standards deployment. COSO is quite well adapted to the global market and its organizations, while ISO 31000 standard works better for companies that have ISO 9001 (2015) quality certification (Dias, 2017). Nevertheless, standards such as ISO/International Electrotechnical Commission ([IEC] 31010, 2009; 2019) help in applying risk identification and risk assessment techniques, as discussed in section 3 regarding the methodology for this research.

To understand the reasons behind the decision to consider COSO as the reference framework for this study, in addition to the ideas mentioned above, we briefly describe the main ISO 31000 standards and the key aspects of the COSO framework, as they are perfectly detailed in their respective documents. Finally, regarding law and regulation bodies we introduce the most relevant commissions supporting risk management practices, as well as the Good Governance Code of Listed Companies Report (Comisión

Nacional del Mercado de Valores) [*National Stock Market Commission*] [CNMV], 2015), and the SOX (2002)[6].

2.1.2.1 ISO 31000 standards

The following is a review of the main contents of ISO 31000 standards (two versions), and ISO/IEC 31010. These standards provide an understanding of the identification and evaluation phases in a risk management process, and the associated techniques in creating a risk identification and assessment model for any type of firm. In this research, the focus is on operational risks, applied to a company in the telecommunications sector (TELCO). As explained above, the processes that follow ISO 31000 standards have not been considered as the most appropriate for this study, because of their complexity of practical application, though they include general processes for risk identification and evaluation; however, it is important to know them: (i) for extrapolating the main concepts applicable to the research (e.g. risk management process identification and assessment steps; and (ii) for the case of organizations where they can be applied in future research. In addition, the study of these standards allows us to appreciate the validity of the process proposed in sub-section 2.1.3, which is part of the objectives of this study. Furthermore, ISO/IEC 31010 standards include the basic techniques that have been used for the methodological development of this research. Finally, the study of risk standards helps knowledge transfer, one of the scientific contribution features of this thesis.

ISO 31000: 2009 Risk Management. Principles and guidelines

Gjerdrum and Peter (2011) provide a clear insight of the main contributions of the international standard on the practice of management titled “Risk Management – Principles and Guidelines” (ISO 31000, 2009). The standard was created by a working group that included subject matter experts from 25+ countries who revised, as a reference, the Australia/New Zealand risk management standard (Standards Australia/Standards New Zealand [AS/NZS] 4360, 2004). This standard can be used by a wide variety of organizations in any country and for any type of operation, regardless of complexity, size or type. Closely related documents are the standards: (i) ISO Guide 73 (2009), which is a compilation of risk-related definitions and terms, and (ii) ISO/IEC 31010 (2009) related to risk assessment techniques (Purdy, 2010).

[6] Both regulations, CNMV (2015) and SOX (2002), are highly interrelated with risk management practices and have impact on TELCO case study.

Considering that the management of risk is central to the livelihood and success of all organizations, the basis for ISO 31000 follows three core pieces of evidence: (i) all organizations exist to achieve their business objectives; (ii) many internal and external factors affect those business objectives, causing uncertainty about whether the organization will achieve its objectives; and (iii) the effect this uncertainty has on an organization's objectives can be managed in terms of risk. One of the key differentiators between TRM (Traditional Risk Management) and this practice of risk management as defined in ISO 31000 is the linking of key risks and the risk management process, as defined in the standard, to an organization's strategic objectives. Furthermore, the standard also includes the possibility to identify and evaluate risks beyond insurable or industrial safety risks, such as reputational and financial risks, expanding the responsibility for managing risk across the organization to a wide range of stakeholders such as "risk owners" (managers) and the staff members responsible for ensuring that risk is effectively managed and evaluated. Also, ISO 31000 (2009) standard is not intended to be specific to any industry or sector. Finally, the key pillars of this standard are the principles, the framework and the process of risk management. ISO 31000 (2009) principles of risk management establish the values and philosophy of the risk management framework and process, supporting a comprehensive and coordinated view of risk that applies to the strategic goals of the entire organization. The main principles establish that risk management:

- creates value and also protects it
- is an integral part of the organization's processes
- is linked to decision making
- manages uncertainty
- is a systematic, structured and timely discipline
- is based on the best available information
- must be adapted to the organization itself
- takes into consideration human and cultural factors
- is transparent and inclusive
- is dynamic, iterative and responsive to change
- favors the continuous improvement of the organization.

The ISO 31000 (2009) standard assists in managing risk effectively, ensuring that information about risk derived from the risk management process is adequately reported and used as a basis for decision making at all relevant organizational levels. The

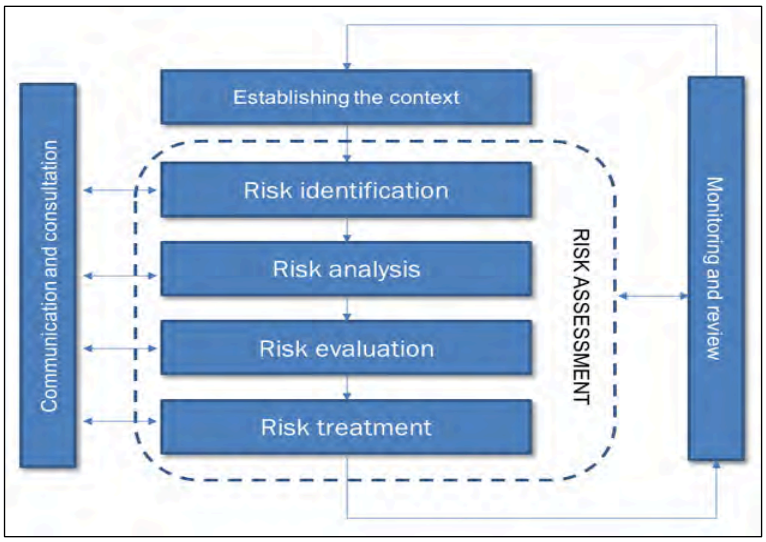
framework assures risk management will be an active component in governance, strategy and planning, management, reporting processes, policies, values and culture.

The component parts of the ISO 31000 (2009) framework are:

- establishing the mandate and commitment to risk management
- designing the framework for managing risk (which includes understanding the organization's internal and external context, establishing a risk management policy, integration of risk management into organizational processes, internal and external communication and reporting and allocation of appropriate resources).
- implementing the risk management process
- monitoring and review of the framework
- continual improvement of the framework.

The ISO 31000 (2009) risk management process, as shown in Figure 2.6, "involves the systematic application of policies, procedures and practices to the activities of communicating and consulting, establishing the context and assessing, monitoring and reviewing risk" (p. 3). The risk management process should be an integral part of management, embedded in the culture and practices, and tailored to the business processes of the organization. These activities are explained in the new version of the standard (ISO/IEC 31000, 2018) as minor differences apply between two editions of the standard, e.g. the classification of the risk assessment set of sub-activities.

Figure 2.6. ISO 31000 (2009) Risk Management Process. Source: ISO 31000 (2009)

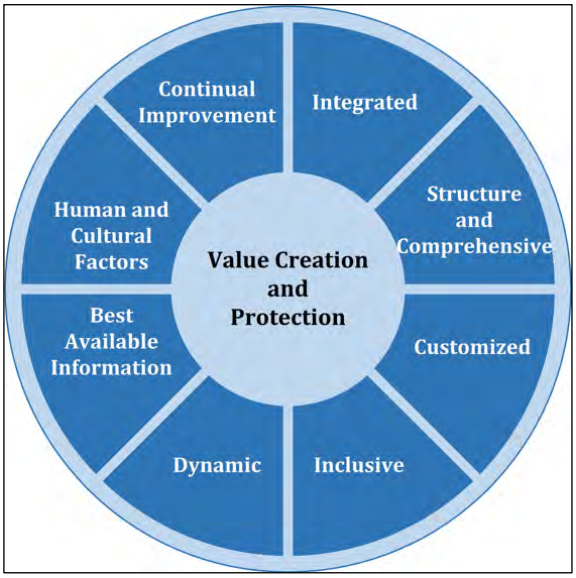


ISO 31000: 2018 Risk Management. Guidelines

As described in the ISO 31000 (2018) standard, titled "Risk Management – Guidelines", the main changes compared to the previous edition ISO 31000 (2009) are the following:

(i) review of the principles of risk management, which are the key criteria for its success; (ii) highlighting of the leadership by top management and the integration of risk management, starting with the governance of the organization; (iii) greater emphasis on the iterative nature of risk management, noting that new experiences, knowledge and analysis can lead to a revision of process elements, actions and controls at each stage of the process; and (iv) streamlining of the content with greater focus on sustaining an open systems model to fit multiple needs and contexts. The ISO 31000 (2018) principles of risk management outlined in Figure 2.7 provide guidance on the characteristics of effective and efficient risk management, being the foundation for managing risk and should enable an organization to manage the effects of uncertainty on its business objectives.

Figure 2.7. ISO 31000 (2018) Risk Management Principles. Source: ISO 31000 (2018)



The elements described as the main principles can be explained as follows: risk management is an integral part of all organizational activities (integrated) with a structured and comprehensive approach which contributes to consistent and comparable results (structured and comprehensive). The risk management framework and process are customized and proportionate to the organization's external and internal context related to its objectives (customized). Also, appropriate and timely involvement of stakeholders enables their knowledge, which results in improved awareness and informed risk management (inclusive). Risks and events can emerge, change or disappear as an organization's external and internal context changes. Risk management anticipates, detects, acknowledges and responds to those changes in an appropriate manner (dynamic). The inputs to risk management are based on historical and current information, as well as on future expectations. Risk management considers uncertainties

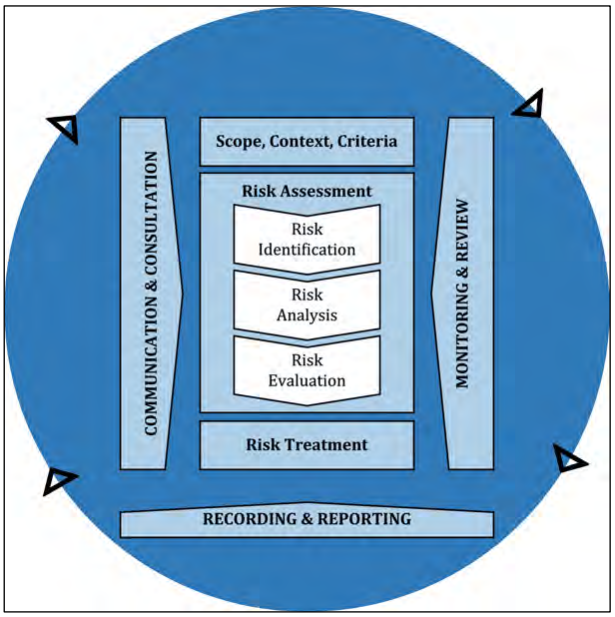
associated with such information and expectations. Information should be timely, clear and available to stakeholders (best available information). Human behavior and culture significantly influence all aspects of risk management at each level (human and cultural factors). And finally, risk management is continually improved through learning, experience and best practices from the academic and business fields (continual improvement). The purpose of the ISO 31000 (2018) framework to assist the organization in integrating risk management into significant activities requires support from stakeholders, particularly from top management. As illustrated by Figure 2.8, the framework development encompasses the following components:

- leadership and commitment, where top management should demonstrate their involvement with the risk management strategy
- integration of risk management into the organization as a dynamic and iterative process
- design in terms of understanding the organization and its context, articulating risk management commitment, assigning organizational roles, authorities, responsibilities and accountabilities, allocating resources, as well as establishing appropriate and timely communication and consultation
- implementation of the risk management framework
- evaluation of the effectiveness of the risk management framework
- improvement for adapting the risk management framework to address changes and continually improve its suitability, adequacy and effectiveness.

Figure 2.8. ISO 31000 (2018) Risk Management Framework. Source: ISO 31000 (2018)

The ISO 31000 (2018) risk management process, as shown in Figure 2.9, involves the "systematic application of policies, procedures and practices to the activities of communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording and reporting risk" (p. 8). The risk management process should be an integral part of management and decision-making and integrated into the structure, operations and processes of the organization. It can be applied at strategic, operational, program or projects levels.

Figure 2.9. ISO 31000 (2018) Risk Management Process. Source: ISO 31000 (2018)



The activities of the ISO 31000 (2018) are described as follows:

- Communication and consultation, the purpose of which is to assist stakeholders in understanding risk for the actions that are required. Communication is about promoting awareness of risk, whereas consultation seeks to obtain feedback and information to support the decision-making processes.
- Scope, context and criteria, when the organization needs to define the scope of its risk management activities (e.g. objectives, expected outcomes, time, locations, appropriate risk assessment tools, resources and responsibilities), the external and internal context, that is the environment in which the organization defines and achieve its objectives (i.e. analysis of risk factors), and risk criteria definition to specify the amount and type to be considered relative to the business objectives (e.g. impact and likelihood definition, how the level of risk is to be determined, the organization's capacity).
- Risk assessment, which is the sub-process comprising risk identification, risk analysis and risk evaluation.

  - The purpose of risk identification is to find and describe risks and categorize them.
  - Risk analysis helps the organization in comprehending the nature of risk and its characteristics, including the level of risk. This activity involves a detailed consideration of risk sources (factors), detailed events, consequences (impact), likelihood (probability of occurrence), and effectiveness of existing controls. It is really the quantification and/or qualification of risks, called evaluation in terms of this study.
  - Risk evaluation involves the results of the risk analysis with the defined risk criteria to support decisions and required actions. It is relevant to note that the name of this activity does not intuitively correspond to the word evaluation, which is one of the reasons mentioned above for not considering ISO as the main frame of reference in this research, in order to help managers of the case study in dealing with the risk discipline and company vocabulary.
- The purpose of risk treatment is the selection and implementation of options for addressing risk. This activity includes two-fold steps: selection of risk treatment options (e.g. avoiding the risk, taking the risk, sharing the risk through contracts or buying insurance, manage/reduce the risk), and preparing and implementing risk treatment plans.
- The purpose of risk monitoring and review is to assure and improve the quality and effectiveness of the risk management process by gathering and analyzing information, sharing results and giving feedback.
- Recording and reporting allow the outcomes of the risk management process to be documented, communicated and reported in order to provide information for decision-making and improve risk management activities.

ISO/IEC 31010: (2019). Risk Management. Risk Assessment Techniques

The ISO/IEC 31010 (2019) standard, the previous edition of which is from 2009, provides guidance on the selection and application of various techniques that can be used to help improve the way risk management processes and models are implemented, which is the case for TELCO. The term “assessment” in the title of the standard includes the two main components of this research: risk identification and risk evaluation (the latter called risk analysis in the ISO 31000 standard terminology).

The main contents of the ISO/IEC 31010 (2019) standard are: (i) techniques for eliciting views from stakeholders and experts; (ii) techniques for identifying risk; (iii) techniques for determining sources, causes and drivers of risk; (iv) techniques for analyzing controls; (v) techniques for understanding consequences and likelihood; (vi) techniques for analyzing dependencies and interactions; (vii) techniques that provide a measure of risk; (viii) techniques for evaluation the significance of risk; (ix) techniques for selecting between options; and (x) techniques for recording and reporting.

As explained in sub-section 3.1.1 (methodology), in the case of this empirical study, the various techniques for operational risk identification and evaluation are: brainstorming, nominal group technique and structured and semi-structured interviews in workshops, surveys through questionnaires, S-curves, Value at Risk (VaR), Monte Carlo simulation, and scenario analysis. The following is a brief description of each technique (the techniques are fully developed in the ISO/IEC 31010 (2019) standard):

- Brainstorming: this tool obtains views from participants so has less need for external information than other methods. Participants need to be, in some way, subject matter experts about the issue they need to discuss. As inputs, it is advisable to have a skilled facilitator for brainstorming to be productive. The outputs are a list of all the ideas generated during the session and the thoughts raised when the ideas were presented. Reference documents are by Goldenberg and Wiley (2011), and Proctor (2014).
- Nominal group technique (NGT): such as brainstorming, and combined with it, this tool elicits the collection of ideas. Views are first sought individually with no interaction between group participants, then are discussed by the group. The inputs are the ideas and experiences of the members, while the outputs are ideas which can lead to decisions as required. The reference document is by McDonald *et al.* (2009). The NGT technique was developed by Delbecq (1968) and it was derived from social-psychological studies of management science.
- Structured and semi-structured interviews: in a structured interview, interviewees are asked a set of questions; a semi-structured interview is similar, but allows conversations to explore issues that may arise. In a semi-structured interview, opportunity is explicitly provided to explore ideas which the interviewee might wish to cover during the interview. The inputs are a clear understanding of the information required and a prepared set of questions (questionnaires). The output is the detailed information required. Reference documents are by Gill and Johnson (2010), and Harrel and Bradley (2009).

- Surveys through questionnaires: they generally engage more people than interviews and usually ask more restricted questions. A survey can involve computer-based questionnaires (as in OpRSA SW for this research). As inputs we can consider unambiguous questions sent to participants. The number of responses needs to be sufficient to provide statistical validity and some expertise is needed in developing a questionnaire in order to achieve useful and appropriate statistical analysis of results. The output is an analysis of the results. The reference document is by Saunders *et al.* (2016).
- S-curves: where a risk might have a range of consequence values, they can be displayed as a probability distribution of consequences. S-curve is understood as a cumulative distribution as a result of plotted data. The probability that a consequence will exceed a particular value can be directly read off the S-curve, being a useful tool when discussing consequence values that represent an acceptable risk. By presenting data in this way, it is easier to see the probability that consequences will exceed a particular value. The inputs are the proposed distributions and associated data. The output is a diagram which can be used in the decision-making process when considering acceptability of a risk, and various statistics from the distribution that can be compared with criteria. This technique is associated with the LDA (Loss Distribution Approach) used in this study. Reference documents are by Garvey *et al.* (2016).
- Value at Risk: Value at risk (VaR) is used in the financial sector to provide an indicator of the amount of possible loss of financial assets over a specific time period within a given confidence level. The distribution of profit and loss is usually derived through Monte Carlo simulation. This approach is particularly useful as it provides information about risks in the distribution tails. The inputs are market factors that affect the value of the portfolio of financial assets, such as exchange rates, interest rates and stock prices. Regarding the output, VaR calculates the potential loss from that portfolio for a specified probability. The analysis is also useful for providing the probability for a specified amount of loss. Reference documents are by Chance and Brooks (2010).
- Monte Carlo simulation: this produces some calculations when analyzing risk distributions. However, performing calculations with distributions is not easy as simulation usually involves taking random sample values from each of the input distributions, performing calculations to derive a result value, and then repeating the process through a series of iterations to build up a distribution of the results. The result can be given as a probability distribution of the value or some statistic

such as the mean value. Systems or sophisticated software tools (as the OpRSA SW for in this research) are used. The inputs to a Monte Carlo simulation are a model of the system with the relationship between different inputs, and between inputs and outputs and the information on the types of inputs, as well as the form of output to be represented. The output could be a single value, or could be expressed as the probability or frequency distribution. Reference documents are by ISO/IEC Guide 98-3 (2008).

- Scenario analysis: this is a range of techniques that involve developing models of how the future might turn out. The input is to undertake a scenario analysis, where data on current trends and ideas for future change are required. The output can be an explanation for each scenario that tells how an organization might move from the present towards the subject scenario. The way scenario analysis has been used in this study is embedded in the OpRSA SW, together with S-curves, VaR/LDA and Monte Carlos simulation of various scenarios. Reference documents are by Chermack (2011) and Ringland (2002).

In this research, the scenario analysis approach, S-curves, Value at Risk (VaR), and Monte Carlo simulation are developed and used in sub-section 3.2.2 when describing the operational risk self-assessment method, and supported by the OpRSA SW tool. It is also important to note that the abovementioned techniques are normally used for firms in the financial sector, being part of the innovation of this research to extrapolate and use those methods for operational risks in the telecommunications industry.

2.1.2.2 COSO frameworks

COSO's mission is to provide thought leadership through the development of comprehensive frameworks and guidance on ERM, internal control and fraud deterrence designed to improve organizational performance and governance and to reduce the extent of fraud in organizations (COSO).

To date, COSO has produced the following main documents: (i) COSO I or COSO (1992) Internal Controls-Integrated Framework which is the framework of complying with section 404 of Sarbanes-Oxley; (ii) COSO II or COSO (2004) ERM, which encompasses COSO I with focus on risk management matters. This framework is widely used by management to enhance an organization's ability to manage uncertainty and to consider how much risk to accept as it strives to increase value within the firm; (iii) COSO III or COSO (2013) is an updated version of COSO I to help organizations design and implement internal

control in light of many changes in business and operating environments since the issuance of the original framework, broaden the application of internal control in addressing operations and reporting objectives, and clarify the requirements for determining what constitutes effective internal control; and (iv) COSO IV or COSO (2017) ERM, the updated version of COSO II for enhancing the framework's content and relevance in an increasingly complex business environment so that organizations can attain better value from enterprise risk management. It recognizes the importance of strategy and entity performance.

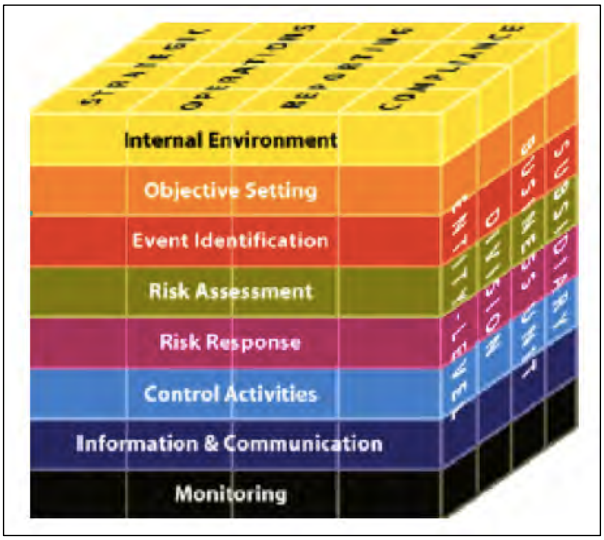
We will focus on COSO II and COSO IV as the reference frameworks for this study, explained as follows. After a detailed analysis of the documents that support the COSO-ERM reports and the ISO 31000 standards, it can be concluded that in both cases, the framework and the standard must be customized for their theoretical and practical application in a company. This characteristic is common and unavoidable in standards; i.e., these management tools represent guidelines for their implementation but rarely fit as a check-list to the deployment objectives of the corresponding models. For example, when a quality management system is implemented based on ISO 9001 (2015), this standard acts as a reference, but the system is specific to each particular organization and its business processes, which will eventually be audited against the standard. Moreover, the COSO framework is even more open in its formulation than the ISO standards, as these structure risk management through a process, which represents an advantage. However, the advantage of the ISO standard's structuring may be undermined by the fact that the organization is too constrained in the application of its contents, even in the language itself, which is sometimes complicated to interpret for a company's managers. It is obvious that whichever option is chosen, it is necessary to implement a risk management process for an adequate deployment of ERM. This is where the opportunity arises to use COSO as a reference framework, and to build a simple and useful risk management process for the organization considering the sequence of its components, which in turn contains the elements under study, as in the case of this research. This is an important proposition that we formulated before starting to create the operational risk identification and evaluation model of this study, and applying it to TELCO.

COSO II: 2004 Enterprise Risk Management – Integrated Framework

COSO II framework (COSO, 2004) provides a practical approach for risk identification and evaluation. This ERM framework is geared to achieving an entity's objectives, set forth in four categories (strategic, operations, reporting and compliance with laws and

regulations) and it consists of eight interrelated components or activities (internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication, and monitoring). As depicted in Figure 2.10, the objectives, activities and organizational units are represented in three dimensions by a cube (the framework). A brief description of each component and objective is provided below. Moeller (2007) is a good reference for clear understanding of COSO (2004).

Figure 2.10. COSO II. ERM-Integrated Framework. Source: COSO (2004)



The components or activities of COSO (2004) are:

- internal environment sets the tone of an organization and its philosophy of risk management and risk appetite
- objective setting aligned with the organization's strategy and consistent with its risk appetite
- event identification of all risks, main component for this research, where operational risks are relevant for the business
- risk assessment, another main component for this study (named as risk evaluation), to consider the extent to which potential events may affect a company's ability to achieve its objectives
- risk response for avoiding, accepting, reducing, or sharing risk
- control activities to ensure that risk responses are carried out
- information and communication to link together each of the other components
- monitoring for the framework to work effectively on a continuous basis.

The categories of objectives of COSO (2004) include:

- strategic (referring to high-level goals, aligned with and supporting the organization's mission/vision)
- operational (where operational risks need to be evaluated; including profitability objectives and referring to the efficiency and effectiveness of the organization's activities)
- reporting or information (referring to the reliability of the information provided by the organization, which includes internal and external data, as well as financial and non-financial information)
- compliance (with applicable laws and regulations).

The two most important components to be considered for this research are event identification and risk assessment (risk evaluation). As summarized by Protiviti (2006), event identification occurs when management identifies potential events that may positively or negatively affect an organization's ability to implement its strategy and achieve its objectives. In general, negative events (such as loss events) represent scenarios that provide a context for evaluating risk and taking actions as risk response, while positive events represent opportunities. Risk evaluation is important to building risk management capabilities for the implementation of models based on COSO-ERM. In fact, as described in the COSO (2004) application techniques document, risk evaluation allows a firm to consider the extent to which potential events have an impact on achievement of business objectives. It is necessary to evaluate events from two perspectives, likelihood and impact, and use a combination of qualitative and quantitative methods, as done in this study. Finally, the key elements of the event identification component to consider are: events, risk factors, event identification techniques, event interdependencies, event categories, and distinguishing risks, and opportunities. The key elements for the risk evaluation component are: inherent and residual risk, establishing likelihood and impact, data sources, assessment techniques, and event relationships.

Finally, we can consider within the COSO (2004) that we have embedded the framework (the cube in its entirety), the process (as abovementioned, the sequence of components or activities, i.e. the front face of the cube), while the principles are attached to every face on the cube, as described in the COSO (2004) executive summary framework (e.g. for the internal environment component there is a section entitled integrity and ethical values). Describing the specific principles in COSO (2004) is the same as describing the

whole framework, due to the fact that those principles are embedded in all its content from the definition of ERM. This is a good approximation; there is no need to speak explicitly of a list of principles, since they are in fact contained in the entire formulation of the framework. As an analogous example, we would have an organization that practices quality without having to continually talk about the term quality in its organization all the time.

COSO IV: 2017 Enterprise Risk Management – Integrating with Strategy and Performance

The COSO IV framework (COSO, 20017) provides greater insight into the value of ERM when setting and deploying strategy, enhancing alignment between performance and ERM to improve the setting of performance targets and understanding the impact of risk on performance. Furthermore, it sets out a framework, components and principles for all levels of management involved in ERM practices.

The reasons for updating the previous edition (COSO, 2004) are related to the following ideas: (i) concepts and practices have evolved with new lessons learned and the "bar raised" with respect to ERM; (ii) business and operating environments are more complex, more technologically driven, and global in scale; (iii) stakeholders are more engaged, seeking greater transparency and accountability; and (iv) risk discussions are increasingly prominent at the board level.

The top changes in the COSO IV framework compared to COSO II are:

- This new framework updates five components (governance and culture, strategy and objective-setting, performance, review and revision, and information, communication and reporting), and adopts 20 clearly stated key principles (explained in detail in the COSO (2017) document) within these five components (governance and culture, strategy and objective-setting, performance, review and revision, and information, communication and reporting) by providing a new document structure, as shown in Figure 2.11. The components are summarized as follows:
    - Governance and culture: governance sets the organization's tone about the importance of risk management, and how culture pertains to ethical values.
    - Strategy and objective-setting: ERM strategy and objective-setting should serve as a basis for identifying, evaluating, and responding to risk. Within

this component, we have COSO (2017) risk management process approach.

- Performance: Risks and events that may impact the achievement of business objectives need to be identified and evaluated, in order to select risk responses.
- Review and revision: the organization needs to understand how ERM components are functioning over time. This should be done by reviewing the organization's performance.
- Information, communication and reporting: ERM should be supported with a continual process of information sharing across the organization.

Figure 2.11. COSO IV. Framework, Principles and Components. Source: COSO (2017)

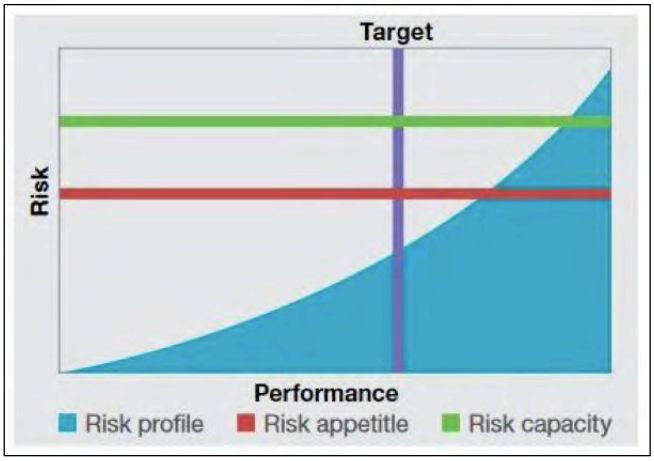
- It incorporates new graphics with stronger ties to the business model and simplifies definitions on risk and ERM, as previously discussed.
- It enhances the focus on how entities create, preserve and realize value, emphasizing it. It embeds value through the new framework as evidenced by its: (i) prominence in the core definition of ERM; (ii) extensive discussion of principles; (iii) linkage to risk appetite; and (iv) focus on the ability to manage risk to acceptable levels.
- It renews the focus on integration by: (i) integrating ERM with other business processes (governance processes, strategy setting, objectives setting, and performance management); and (ii) really focusing on applying ERM at various levels of the organization (e.g. entity level, business unit, division).

- It recognizes the importance of culture, examining its role by: (i) addressing the growing focus, attention and importance of culture within ERM; (ii) exploring the relationship with culture in the context of risk governance, oversight of the entity and connection between framework components; (iii) depicting the behavior within a risk spectrum from risk averse to risk aggressive, with the possibility of being risk neutral in the middle; (iv) affecting the entity's decision making; and, (v) exploring the alignment of culture between individual and entity behavior.
- It elevates discussion of strategy by: (i) exploring ERM and strategy from three different perspectives; (ii) analyzing the possibility of strategy and business objectives not aligning with mission, vision and values; and (iii) considering the risk to executing the strategy. ERM is as much about understanding the implications from the possibility of strategy not aligning as it is about managing risks to set goals (COSO, 2017). Figure 2.12 illustrates these aspects in the context of mission, vision, core values, and as a facilitator of an organization's performance.

Figure 2.12. COSO IV. Strategy in Context. Source: COSO (2017)

- It enhances alignment with performance by: (i) enabling the achievement of business objectives by actively managing risk and performance; (ii) focusing on how risk is integral to performance by exploring how ERM practices support the identification and assessment (evaluation) of risk that impact performance; and discussing acceptable variations in performance; (iii) managing risk in the context of achieving business objectives not as individual risks; (iv) seeking to enhance the integrated reporting on risk and performance; (v) introducing a new depiction referred to as a risk profile (as shown in Figure 2.13) and how to build it, incorporating the concepts of risk, performance, risk appetite and risk capacity; and, (vi) offering a dynamic and comprehensive view or risk and enabling more risk-aware decision making.

Figure 2.13. COSO IV. Risk Profile. Source: COSO (2017)



- It links into decision making by: (i) exploring how ERM drives risk aware decision making; (ii) highlighting how risk awareness optimizes and aligns decisions impacting performance; and (iii) exploring how risk aware decisions affect the risk profile.
- It delineates between ERM and internal control. COSO IV does not replace COSO III (COSO, 2013). Both frameworks: (i) are distinct and complementary; (ii) use components and principles structure; (iii) have aspects of internal control common to ERM that are not repeated; and (iv) are written in a way that aspects of internal control are developed further in this COSO IV (COSO, 2017) framework.
- It refines risk appetite and acceptable variation in performance by: (i) including the risk appetite definition in terms of amount of risk, organization willing and value, as previously described; and (ii) defining acceptable variation in performance in terms of the boundaries of acceptable outcomes related to achieving business objectives (COSO, 2017).

In summary, as stated by the project update goals to produce the COSO (2017) standard, we have available an updated ERM framework that: (i) provides insight into strategy and the role of ERM when setting and executing it; (ii) enhances alignment between performance and ERM; (iii) accommodates expectations for governance and oversight; (iv) recognizes globalization and the need to apply a common, albeit tailored approach; (v) presents new ways to view risk in setting and achieving objectives in the context of greater complexity; (vi) expands reporting to address greater transparency; and (vii) accommodates evolving technology and new practices.

Furthermore, as we anticipated, and in practical terms for the purpose of this research, considerations from COSO frameworks in terms of risk identification and risk evaluation are better treated than in ISO 31000 standards. It is important to note that even in two out of five components of COSO (2017), risk identification and risk evaluation are highlighted as core activities for a successful implementation of ERM.

2.1.2.3 Law and regulation commissions

In addition to COSO, other various commissions and task forces were created for the development of risk management (Simkins and Ramirez, 2018; Kloman, 2010) such as the Cadbury report (Cadbury, 1992), which suggests the responsibility of the board of directors for the enterprise risk management policy, the Hampel report (Hampel, 1998), which through the Committee of Corporate Governance states the responsibility of directors for setting up a risk management system capable of identifying, assessing and managing major risk to the enterprise, the Turnbull code[7] (Turnbull, 1999), which highlights the key role for internal control in monitoring the effectiveness of the risk management system, and the Conthe code (Conthe, 2006), led by the president of Spain's National Stock Market Commission (CNMV-*Comisión Nacional del Mercado de Valores*) at that time, who presented at the Madrid stock exchange the outlines of a code of good governance including the company's policies and strategies for risk control and management, where risk management policy should specify at least: (i) the different types of risk (operational, technological, financial, legal, and reputational) the company is exposed to; (ii) the determination of the risk level the company sees as acceptable; (iii) measures in place to mitigate the impact of risk events; and (iv) the internal reporting and control systems to be used to manage risks. This code was updated in the document Good Governance Code of Listed Companies report (CNMV, 2015), stating that the company should maintain a risk control and management function in the charge of an internal unit or department, supervised directly by the audit committee or, where appropriate, another dedicated board committee, in addition to the abovementioned elements of the risk management policy. Furthermore, the Institute of Internal Auditors adopted a new definition of internal auditors that includes risk management roles (Ramamoorti, 2003), stating that internal auditing should help an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes (IIA, 2004). All these codes and corporate good governance rules, as well as SOA Law, are

[7] In October 2005 the document "Internal Control: Revised Guidance for Directors on the Combined Code" was issued, which is based on and very similar to the Turnbull guidance.

considered as administrative obligations more than practical approaches for implementing an enterprise risk management system in companies, and this is the main reason why the COSO II and COSO IV frameworks, as well as ISO 31000 standard (Kloman, 2010), have been chosen as the reference models for this research study, being suitable approaches with the purpose for risk identification and management.

Furthermore, both the Good Governance Code and the Sarbanes-Oxley Act, explained below, are applicable to TELCO as it is part of TELCO Group which is a SEC registrant company in New York and listed in CNMV in Madrid.

Good Governance Code

The concept of good governance has existed for almost a century; however, it was in the 1970s, with the consolidation of global financial markets and the gradual adoption of neoliberalism, that the term began to gain greater popularity. The purpose of strengthening the concept of Corporate Governance (CG) in a systematic manner was to guarantee investors the necessary transparency and proper management of companies and that all this would result in the continuous improvement of companies.

As a business practice, it is said that a company without corporate governance is like a body without a conscience. International experience has shown that the adoption of better corporate governance practices within organizations is closely related to their transcendence and sustained growth. These practices are aimed at all types of companies, from the newly created to those listed on the stock exchange. The degree of maturity that companies have in decision making and business management is related to the adoption of corporate governance practices that generate more value to the organizations considering their priorities. From a public perspective, there are several international organizations working to promote global principles of good governance, such as the OECD (Organization for Economic Cooperation and Development) and the World Bank through the International Finance Corporation (IFC).

As explained by the Organization for Economic Cooperation and Development ([OECD], 2014), corporate governance is a key element in increasing economic efficiency and growth potential, as well as in fostering investor confidence by facilitating effective oversight of the bodies within the company. Other institutions also provide inputs regarding corporate governance, such as the Mexican stock exchange which describes corporate governance as the framework of rules and practices, which refer to the structures and processes for the management of companies, by which a board of

directors ensures accountability, fairness and transparency in a company's relationship with all its stakeholders (the board of directors, shareholders, customers, employees, government and the community). In fact, corporate governance can be understood as the system under which companies are managed and controlled.

Corporate governance goes beyond looking after the interests of investors. The latest trends associated with transparency, accountability and corporate responsibility are extending this scope to the management and treatment of financial and, additionally, non-financial information with other stakeholders. For this reason, and as the 3rd corporate governance survey from PwC Mexico describes, corporate governance is being given greater relevance and focus on its value and contribution to business for the following reasons: (i) the relevance of transparency and sustainability issues in recent years has increased the interest of organizations to expand the concept of corporate governance to more stakeholders, and not only limit it to investors (employees, government, society, customers, partners); (ii) sometimes, depending on the sector-industry of the company, other stakeholders are more important than the investors themselves for the development and success of the business; and (iii) the impact that social and environmental management issues have on society and / or the community for the development of the business (third-party management, human rights, climate change) is of increasing value. Furthermore, corporate governance obeys universal principles, but it must be different and unique to adapt to each company's singularity and the level of maturity reached by the practices of its senior management.

Regarding the relation between risk management as the Good Governance Code of Listed Companies report (CNMV, 2015), which is the case with TELCO, these are the main contents in terms of principles and recommendations:

- Principle 21: "The company should maintain a risk control and management function…" (p. 36).
- Recommendation 45: "Risk control and management policy should identify at least:
    a) The different types of financial and non-financial risks the company is exposed to…
    b) The determination of the risk level the company sees as acceptable.
    c) The measures in place to mitigate the impact of identified risk events should they occur.
    d) The internal control and reporting systems to be used to control and manage the risks…" (p. 36).

- Recommendation 46: "…risk control and management function…charged with the following responsibilities:
    a) Ensure that risk control and management systems are functioning correctly…and the major risks…are correctly identified, managed and quantified.
    b) Participate actively in the preparation of risk strategies and in key decisions about their management.
    c) Ensure that risk control and management systems are mitigating risks effectively in the frame of the policy drawn up by the board of directors." (p. 37)

The Sarbanes-Oxley Act (SOA or SOX)

The United States Congress passed the Sarbanes-Oxley Act (SOA or SOX) in 2002. It established rules to protect the public from fraudulent or erroneous practices by corporations and other business entities. About the history of SOX compliance, senator Paul Sarbanes and representative Michael G. Oxley wrote this bill in response to several high profile corporate financial scandals – Enron, Worldcom and Tyco, in particular, among many others where financial frauds deceived the stakeholders by promising high dividends for something that was worth nothing at all (Anomaly and Brennan, 2014; Donaldson, 1995; Merton and Peron, 1993). The stated goal of SOX is to protect investors by improving the accuracy and reliability of corporate disclosures (SOX, 2002). The bill established responsibilities for boards and officers of publicly traded companies and set criminal penalties for failure to comply. SOX established rules to protect the public from fraudulent or erroneous practices by corporations and other business entities. The goal of the legislation is to increase transparency in financial reporting by corporations and to require a formalized system of checks and balances in each company. SOX compliance is not just a legal obligation but also good business practice. SOX applies to all publicly traded companies in the United States as well as wholly-owned subsidiaries and foreign companies that are publicly traded and do business in the United States.

The most important SOX compliance requirements were summarized by Peters (2020) as follows:

- CEOs (Chief Executive Officers) and CFOs (Chief Financial Officers) acknowledge responsibility for the accuracy, documentation, and submission of all financial reports, plus the internal control structure to the SEC (Security

Exchange Commission). Officers risk jail time and monetary penalties for compliance failures – intentional or not.

- SOX requires an internal control report that states management is responsible for an adequate internal control structure for their financial records. Any shortcomings must be reported up the chain as quickly as possible for transparency.
- SOX requires formal data security policies, communication of data security policies, and consistent enforcement of data security policies. Companies should develop and implement a comprehensive data security strategy that protects and secures all financial data stored and utilized during normal operations. COBIT (The Control Objectives for Information and Related Technology) is another framework to implement SOX compliance developed by ISACA (Information Systems Audit and Control Association). It is a comprehensive list of 34 best practices for IT security. ITGI (The Information Technology Governance Institute) is another IT framework to achieve SOX compliance. ITGI uses standards from both COBIT and COSO, but ITGI focuses on security instead of just focusing on general compliance.
- SOX requires that companies maintain and provide documentation proving they are compliant and that they are continuously monitoring and measuring SOX compliance objectives.

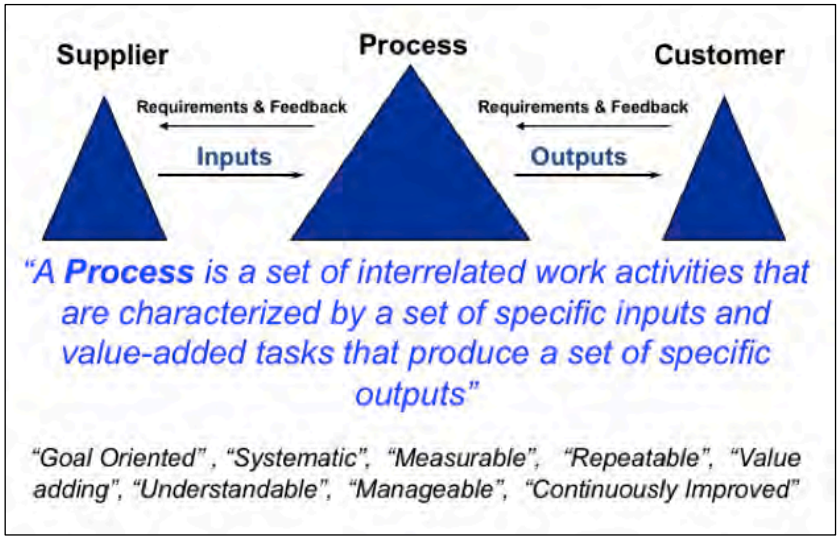
SOX Section 404 (management assessment of internal controls), which is the case for TELCO, requires that all annual financial reports must include an internal control report stating that management is responsible for an adequate internal control structure, and an assessment by management of the effectiveness of the control structure. In addition, registered external auditors must attest to the accuracy of the company management assertion that internal accounting controls are in place, operational and effective. Regarding risk management, it requires that listed companies use an internal assessment control framework (e.g. COSO – The Committee of Sponsoring Organizations of the Treadway Commission). Additionally, SEC (Security Exchange Commission) and PCAOB (The Public Company Accounting Oversight Board) have issued new regulations for risk assessment (e.g. TDRA SOX Top-Down Risk Assessment).

2.1.3 A framework for the risk management process

Once the risk management processes associated with ISO standards and ERM frameworks have been studied, the risk management process selected for this research applied to TELCO will be inspired on the contents of the theoretical foundation (particularly on COSO II for the reasons explained) and the references and models described below. In summary, it is a matter of choosing a lean, useful and practical risk management process, which allows visualization and application of the phases of identification and evaluation of operational risks, which are the objective of this study.

First, we need to agree on a definition of process: “a process can be defined as a set of interrelated activities...that transfer a useful outcome to the internal or external customer” (Ruiz-Canela López, 2004) (p. 326). In this definition we consider that a set of activities or tasks to be defined as a process need to have the following characteristics: (i) goal oriented; (ii) systematic; (iii) measurable; (iv) repetitive over time; (v) value adding; (vi) understandable when explained or documented (not “rocket science”); (vii) manageable; and (viii) susceptible to be continuously improved. This also applies to risk management processes. All these ideas are summarized in Figure 2.14.

Figure 2.14. Concept of Process



The risk management process takes the company’s strategy and objectives as the basis for identifying the main risks that could affect these objectives. Risks are identified and evaluated by managers in order to prioritize their reporting and follow-up, but especially to determine the response to them, generally through mitigation plans, or strategies to avoid or transfer such risks. This process is usually carried out by the risk managers, who are, in turn, the managers of the different functions in the companies at the local level, and the global or corporate managers to whom they report. The risk management

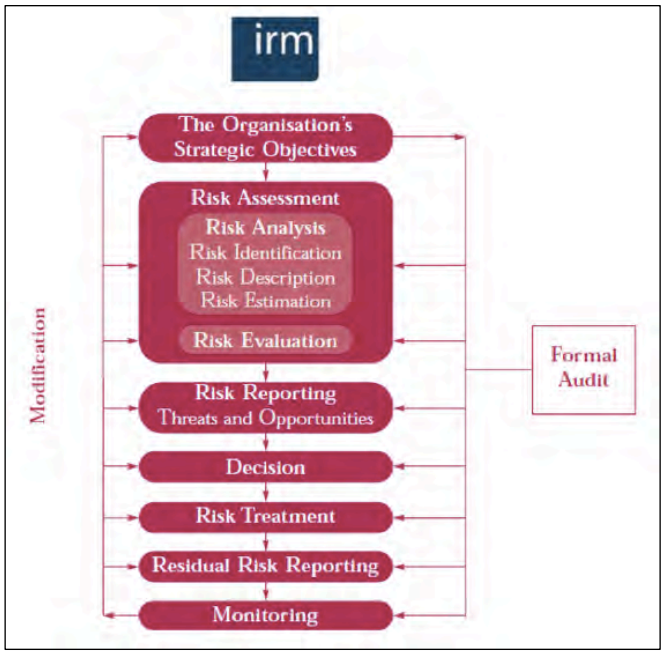
function that may exist in a large organization supports the risk managers in the execution of the process.

In addition to the risk management processes studied on the basis of ISO, there are other models, such as EFQM (2005), which propose activities similar to those already studied. In this case, the EFQM Basic Risk Management Process includes the following phases:

- Risk recognition which integrates context establishment and risk identification.
- Risk prioritization which includes risk analysis (qualitative and quantitative methods) and risk evaluation (with a scale to give a ranking; i.e. low or tolerable, medium which is tolerable if the risk is reduced to be "As Low As Reasonably Practicable" – ALARP – and high or intolerable).
- Managing risks with decisions (terminate-avoid or eliminate the loss exposure, treat-risk and loss control activities, tolerate-acceptable level of risk, and transfer-sharing the impact through insurance) and implementation steps.
- Monitoring and review which is interrelated with the three previous phases.

Also, IRM (2002) standard proposes a risk management process very similar to the abovementioned based on ISO standards, COSO frameworks and EFQM model. The main elements are shown in Figure 2.15. IRM (2002) is a simple guide that outlines a practical and systematic approach to the management of risk for business managers as well as for risk professionals.

Figure 2.15. IRM Risk Management Process. Source: Institute of Risk Management (IRM)

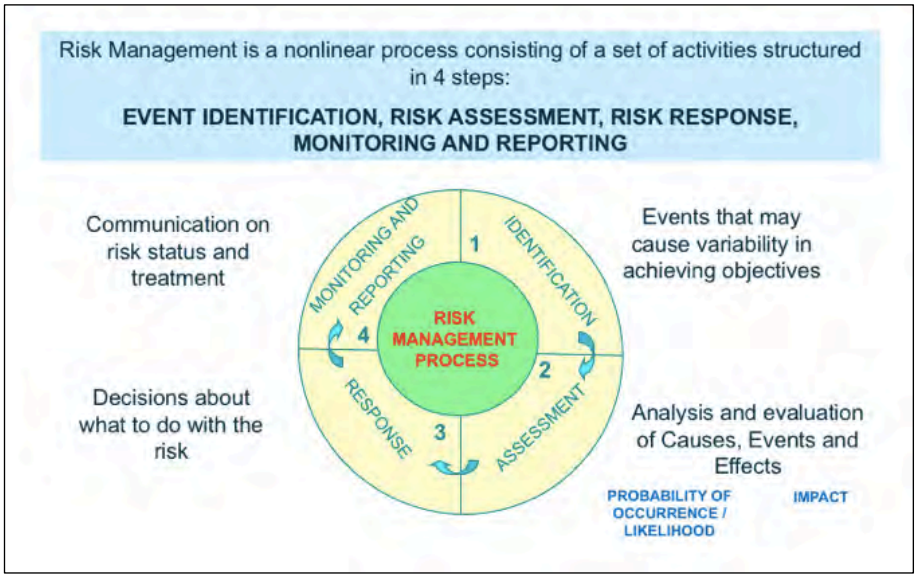


Chapman (2008) provides a complete description of the six stages of the risk management process based on the IDEFO (Integration Definition for Function Modelling) technique, including: (i) analyzing the business; (ii) risk identification; (iii) risk assessment; (iv) risk evaluation; (v) risk planning; and (vi) risk management of the process. In some ways, this risk management process approach is similar to the ones described by ISO 31000.

Again, in both models (EFQM, IRM), what would intuitively, in plain language, be risk evaluation is treated as risk analysis. In contrast, in the IDEFO model, risk evaluation is understood as risk assessment.

Based on all the analyzed and most relevant risk management processes existing so far, this study proposes the following risk management process shown in Figure 2.16. This risk management process is simple, useful and practical for the objectives of this research. The four main steps in a risk management process are: (i) event identification; (ii) risk assessment or evaluation; (iii) risk response; and (iv) monitoring and reporting.

Figure 2.16. Risk Management Process Steps



- Event identification: the objective of this first step of the risk management process is to anticipate the potential risks that might affect the achievement of the company's strategic objectives through the assessment of the affected processes. The risk identification will allow the organization make an integral vision available about them in order to facilitate the monitoring and anticipation of negative effects. Risks must be identified in terms of both the factors that cause them and the effects they may have on the achievement of certain objectives. Within a period, the following can be identified:

- Risks already existing and reported in previous periods.
- New risks, those risks that did not exist in the previous report.
- Materialized risks, events occurring in relation to previously reported or non-reported risks.
- Emerging risks, those risks that could potentially have an adverse impact on the company's future performance, although their outcome and time horizon is uncertain and difficult to predict.

Figure 2.17 illustrates an example of classification at different levels of an identified event as a potential risk ("end customer and sale of products and services").

Figure 2.17. Event Identification. Illustration

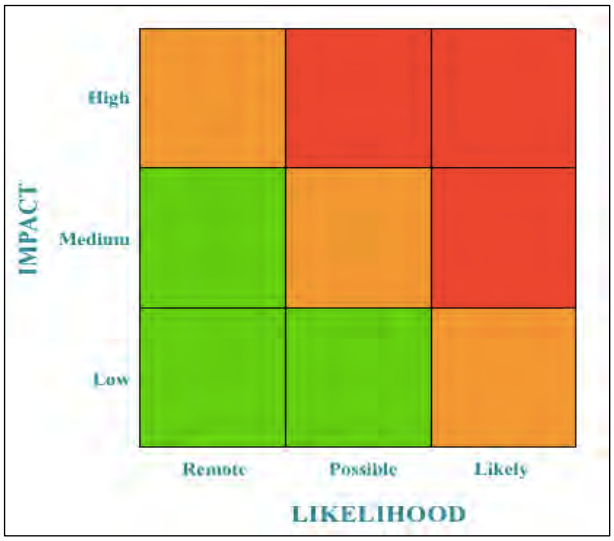
EVENTS MODEL					
Event (Level 1)		Category (Level 2)			Category (Level 3)
1	**End Customer and Sale of Products and Services**	1.1	End Customer	1.1.1	Customer data protection claims
				1.1.2	Claims relating to performance/provision of the service (breakdowns, breach of other service levels, quality standards, etc., excluding claims regarding measurement/charging/billing)
				1.1.3	Claims relating to measurement/charging/billing/collection/product or service not recognized
				1.1.4	Claims relating to the customer attention service (actual and potential)
		1.2	Marketing and sale of Products and Services	1.2.1	Errors or inaccuracies in the information given to customers
				1.2.2	Errors in capture, recording and maintenance of information used to design products, offers, solutions, prices, services and marketing campaigns
				1.2.3	Errors in identifying, planning and/or launching products, services, solutions, offers and marketing campaigns
				1.2.4	Errors in the design of products, services, offers, solutions marketing campaigns (including loyalty programs)
				1.2.5	Errors/inaccuracies in information recorded on customers/products and/or services contracted
		1.3	Customer service	1.3.1	Error, failure or poor quality in Customer Attention (actual and potential) including post-sale service

- Risk assessment (evaluation): the objective of this second step of the risk management process is to know the impact dimension of the potential events (risks) for the achievement of the company's objectives. Through risk assessment, the company can obtain a measure of the economic impact and probability of occurrence of the identified risks. The impact is defined as the potential loss that each risk may cause if it materializes and is measured, in general, with a specific time horizon (e.g. one year). For its estimation, it may be convenient to count on the support of the various areas of the company, particularly, finance, management control and auditing areas. Key elements to measure a risk are:
  - probability of occurrence (likelihood): level of certainty about the risk realization

- risk impact: potential loss that the risk could lead to the achievement of the company objectives
- risk heat map: graphical tool which enables the company to understand the evaluated risk in a visual way (in terms of impact and likelihood). It is useful to have the information of risk heat maps detailed in risk register templates, including various concepts to identify and assess the risk, such as risk category, probability, impact, risk response and risk owner.

Figure 2.18 illustrates an example of a risk heat map to plot the risks against likelihood or probability of occurrence and consequence or impact variables. The risk heat map is an effective tool for communication to management, and useful for an appropriate risk prioritization. There are alternative scales for the risk heat map variables such as: impact (very high or critical, high or major, medium or moderate, low or minor, and very low or insignificant) and likelihood (very likely or almost certain 81-100%, likely 51-80%, very possible 31-50%, possible or unlikely 11-30%, and remote or rare 0-10%).

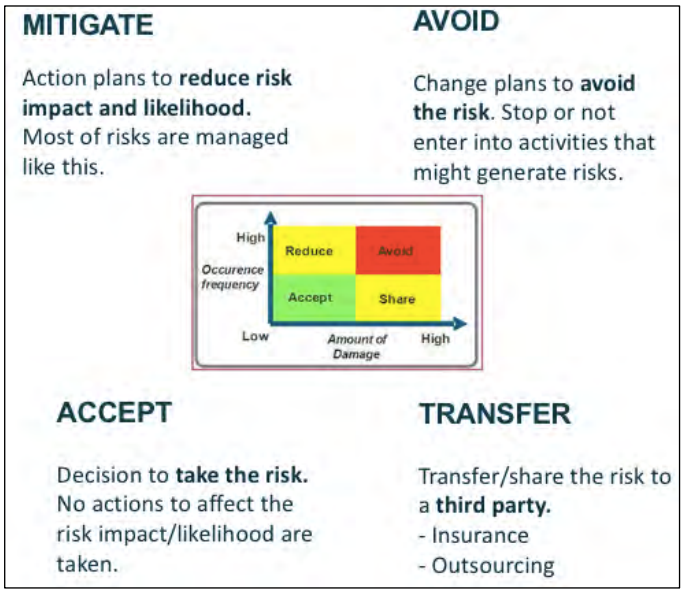
Figure 2.18. Risk Heat Map. Illustration



- Risk response: the objective of this third step of the risk management process is to establish the necessary actions for risk response, once they have been previously identified and evaluated. The company needs to determine the most appropriate answer used to involve a cost-benefit analysis on the required actions. The actions to be taken by managers and/or those responsible for the mitigation plans are established as a response, in order to minimize the effect of the risk, for which implementation dates and responsible parties are established.

The different types of risk response are shown in Figure 2.19 and described below:

Figure 2.19. Risk Response Types

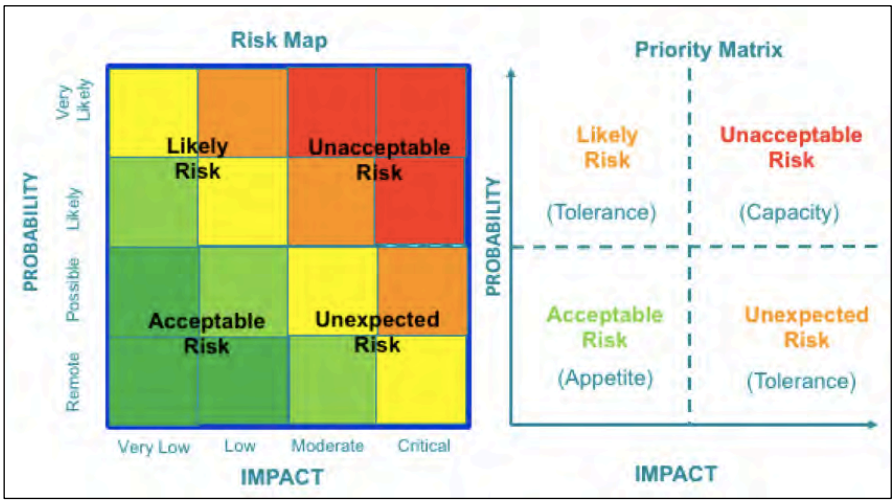


- Avoid/terminate: changing the way of acting or not proceeding with the activity that causes the risk.
- Mitigate/treat: most risks are managed in this way. It consists of taking measures to reduce the probability of occurrence of the risk, its potential impact, or both. Action plans are designed and organized.
- Transfer: share some or all of the risks to a third party, for example by taking out insurance or outsourcing activities. In the latter case it will be very important to ensure contractually and operationally that the risks have been effectively transferred to the supplier.
- Accept/tolerate: take the decision to assume some risk based on management criteria (e.g. due to too high mitigation costs). This decision must be made at the appropriate level within each organization, and must be properly justified and documented. It is important to monitor the risk to ensure that the risk exposure has not changed. As a general rule, this response to risk involves not implementing action plans.

- Monitoring and reporting: the objective of this fourth step of the risk management process is to conduct follow-up and monitoring of the risks, as well as reporting the status of the risk portfolio of the company and the actions plan's effectiveness. For each risk identified and reported in the period, a mitigation plan must be established with a responsible party and an implementation date agreed (except if the risk is "accepted", in which case it does not have a mitigation plan). In the

following periods, its follow-up and degree of progress must be updated and reported. Likewise, the risk owners (managers) must identify the priority risks to be monitored within its scope in order to update their evolution. Figure 2.20 illustrates how risks are reported, as well as the relationship between the zones where these risks are located and the concepts of appetite, capacity and tolerance associated with them.

Figure 2.20. Risk Monitoring and Reporting. Illustration



Large companies such as TELCO have robust IT tools for risk management (e.g. OpRSA SW), which generate information for risk monitoring, including detailed reports and graphs.

As described, it is possible to design a lean, useful and practical risk management process applicable to a company, regardless of its complexity. This research study is focused in detail on the first two steps of the risk management process, identification and evaluation applied to operational events at TELCO (the steps related to the research propositions as described in sub-section 2.5). The empirical results also provide insights for the third step (risk treatment).

2.2. Previous studies on operational risks identification and evaluation

Starting with the literature review, the concept of ERM began to take root in the late 1990s and has since created positive expectations for effective management and good corporate governance. However, as evidenced by research, such as the study of Fraser and Simkins (2016) applied to a best practice business case in risk management deployment, many companies belonging to different sectors still struggle with ERM implementation. Nevertheless, over the last two decades, the ERM approach has gained substantial momentum, and many firms (mainly from the financial sector) have

implemented risk management processes for risk identification, evaluation, and management. Despite its growing experience in practice, ERM frameworks have attracted little attention to research compared to other disciplines. In fact, the concept of risk has been related by authors such as Knight (2006) to the concepts of profit, uncertainty and competition in related disciplines such as economic theory. However, the relevant literature on specific ERM-related issues has been developed and has inspired this study. In order to initially understand the overall context of this research, it has been necessary to review the following: one set of papers that examines the factors that influence ERM adoption (Beasley *et al.*, 2005; Kleffner *et al.*, 2003; and Liebenberg *et al.*, 2003); other research works that study the effects of ERM adoption on performance (Beasley *et al.*, 2008; and Gordon *et al.*, 2009); as well as another cluster of papers that explores risk management practices in specific organizational settings (Mikes, 2009; Wahlström, 2009; and Woods, 2009). As studied by Nocco and Stulz (2006), a carefully designed ERM approach can be a source of long-run competitive advantage through its effects both macro or company-wide level (i.e., enabling senior management to identify, measure, and manage to acceptable levels the risks faced by the firm) and micro or business-unit level (e.g., adding value by ensuring that relevant risks are efficiently evaluated by operating managers and employees throughout the company).

The ERM framework is oriented towards an integrated management of all the risks of a company. Within this general concept of ERM, numerous risk classifications have been suggested, one of which distinguishes between market (financial), credit, business and operational risk. One of the essential tasks when starting the implementation of an operational risk management model is usually to agree on the definition of operational risk in order to limit and determine its scope. According to Lewis (2006), a possible definition of operational risk could refer to potential losses of value or results arising from events caused by inadequacies or failures resulting from processes, human resources, physical equipment and IT systems or from external factors. This definition includes compliance risk, but excludes strategic and regulatory risk. Typically, operational losses include economic, non-economic and reputational effects. More precisely, it can be reasoned that operational risk is related to any risk arising from the companies' business activities and the practical implementation of the management strategy. This concept is broad, and includes information risks, fraud risks, physical or environmental risks. Another way of understanding it would be to define it initially as any form of risk that is not market or credit risk. However, this definition is not very rigorous because it does not define exactly the types of risk that banks and other firms currently face, nor does it

provide a formal basis for identifying and measuring risk, and calculating capital requirements (Cruz, 2005). A specific definition, provided by BCBS (2008), defines operational risk as the risk of loss that occurs as a result of inadequate or failed internal processes, as well as external events.

The definition of operational risk in terms of possible losses of value or results derived from events caused by inadequacy or failures arising from processes, human resources, physical equipment and computer systems or derived from external factors, contrasts with and allows differentiation from other general types of risks, such as business, financial or credit risks. Some of these are: (i) business risk would correspond to losses in value or results arising from strategic uncertainties, changes in the environment and market, competition or due to alterations in the regulatory framework (e.g. threat of a new competitor or a technological change); (ii) with respect to financial (market) risks, potential losses would be associated with adverse movements in financial variables and the company's inability to meet its commitments or make its assets liquid (e.g. exchange rate fluctuation); and (iii) credit risks deriving from the failure to pay or deliver on contractual payment obligations of the company's counterparties (e.g. customer delinquencies). However, this is a very open classification, and in each case, depending on the sector and the type of company, it is necessary to differentiate between the conceptual differences in the nature of each type of risk. In fact, operational risks can be characterized by the following attributes (Ashby, 2008): (i) they are inherent to the business and therefore related to most of its activities; (ii) they are specific, in the sense that all the measures to control and mitigate them depend on the specific risk profile of each company; and (iii) they are closely related to the culture and practices of the business where they apply. However, this does not prevent the existence of interrelationships between the different risk categories described; in fact, the occurrence of operational events may be causes for the materialization of financial risks or commercial credit risks (e.g. the failure of a computer system could affect the ability to collect debts from customers). In fact, BSI 31100 (2007) includes market risks, credit risks, operational risks, project risks, financial risks, strategic risks and reputational risks as generic categories, clarifying that the categorization of risks may be influenced by legal and regulatory requirements, as well as by industry practices. In principle, a correct extrapolation of the definition of operational risk in the financial sector for its application to telecommunications companies[8] could be valid, provided that the characteristics that, according to Ashby (2008), differentiate the management of this risk between financial

[8] As in the case study of this research (TELCO).

and non-financial entities are taken into account: (i) the root causes of operational losses in non-financial companies are more organizational than due to purely technical factors; (ii) the causes of operational losses for non-financial companies are usually multiple and interrelated, not typically due to an isolated factor (in the case of financial entities, such as the failure of an IT system); and (iii) operational risk management is not only related to loss prevention or the reduction of financial loss via insurance or capital provisioning. For the proper management of operational risk, especially in non-financial entities, it is necessary to invest in capabilities and management models that allow minimizing, in case of risk materialization, costs and discontinuities in the supply of the product or in the provision of the service. The characteristics described above will be considered for a correct formulation of the concept of operational risk in a telecommunications environment.

In relation to the challenge posed by operational risk management in the business environment, there is currently a great deal of knowledge already developed in this area for the financial sector, mainly due to the challenges presented in the new regulations created in Basel II (BCBS, 2006). The management of this type of risk is gradually becoming a relevant fact within the practice of risk management in financial markets and has been evolving from an approach based on regulatory compliance to its use within the basic parameters of banking business management. In addition, interest and research in operational risk is growing rapidly in non-financial sectors because it represents one of the major sources of risk in industries where continuity and quality of service are key, such as in telecommunications companies. This industry is considering it critical to overcome this challenge, which would require adding to the methods traditionally used, new models for the identification, measurement, management and improvement of this operational risk, which is the subject of this research. The ultimate goal would be to reduce the costs of its operational processes and the minimization of economic losses derived from the materialization of operational risks and the optimization of existing controls, as well as other benefits that can be derived from the implementation of ERM models, as described in this study.

According to COSO (2004), many companies are trying to define the basis for a practical, efficient and value-generating implementation of the risk management principles established in internationally accepted references. In this sense, companies often include operational risk management as part of their ERM models, which consist of a set of organizational measures that, by acting in a coordinated manner, help to make risk management more efficient throughout the organization. In this way, an ERM approach

becomes a key element for the creation of value in a company, as a systematic risk/benefit analysis is carried out on an ongoing basis throughout the company, from the board of directors to the day-to-day management of operations. These practical and efficient implementations consider that operational risk must be a key element of the risk models (the only way, for example, to really respond to the objective of effectiveness and efficiency of the companies' operations), and must have a method adapted to the nature and behavior of operational risk, which captures the importance of the economic and human resources that companies devote to the management of their operational processes and risks (e.g. investment costs, operation and maintenance of facilities, insurance, indemnities, and fines). Moeller (2007) and Cendrowski and Mair (2009) provide a complete review of ERM and COSO (2004).

The challenge of operational risk management corresponds precisely to its application in non-financial or industrial sectors, which should respond in their performance to criteria of value generation for business management and not so much to compliance with certain regulatory obligations, as is the case of financial institutions with respect to the Basel Accords (BCBS, 2006). This challenge becomes even more evident when understanding the lessons learned in operational risk for non-financial organizations. According to Ashby (2008), the efficient management of operational risk is both an art and a science, due to the fact that professionals dedicated to these functions have to know how to manage social, cultural and human factors of the organization, in addition to those typically proposed by financial institutions, such as process failures, system failures or external factors, among others (BCBS, 2004). According to Knop *et al.* (2004), risk measurement has become a basic function for the correct capital management of companies, especially those in the financial sector; a basic question that has not been fully answered is how to apply these techniques to non-financial sectors.

In fact, the discipline of operational risk management has been maturing for decades within the financial sector, supported by regulatory initiatives such as the abovementioned Basel Accords, and business factors due to increasing competition, improved risk-based decision making and value creation for stakeholders. Major strides for this sector have been developed in areas such as risk identification and evaluation and loss data collection in line with the main objective of the Basel II Accord, which is to improve the stability and soundness of the international banking system, in particular by enhancing risk management practices and developing significantly more risk-sensitive capital requirements (BCBS, 2006).

The Basel II Accords (named after the city where it was approved) allows the capital requirement to be lowered. Basel II is established as a general principle that any company must have a protection fund (self-insurance) for the financing of the risks to which it is exposed, housed in its capital. This portion of capital is called regulatory capital. It also establishes the capital requirements necessary to ensure the protection of companies against financial and operational risks. Its purpose is to standardize processes within financial and business operations to mitigate risks. To understand the Basel II framework, let us first analyze the following concept: operational risk was understood as everything that was neither credit risk nor market risk. BCBS (2003), as a starting point in the management and control of operational risk, standardizes the concept of operational risk, defining it explicitly in BCBS (2004) as the risk of loss resulting from an inadequacy or failure of internal processes, personnel and systems or from external events. This definition includes legal risk, but excludes strategic risk and reputational risk. The risks regulated by BCBS (2002) are operational, credit and market (financial) risks. The above definition of operational risk refers to losses. The types of loss exposures (negative events) include: internal fraud, external fraud, labor relations and workplace safety, customer, product and professional practices, damage to tangible assets, business incidents and systems failures, as well as process execution, delivery and management; credit risk corresponds to the risk assumed by the lender arising from the possibility that the borrower will default on its obligations; and market risk is defined as the risk of losses arising from movements in market prices. This includes risks pertaining to financial instruments related to interest rates, exchange rates, as well as risks related to share prices. In addition to this contribution on the definitions and classification of risks, Basel II describes the so-called fundamental pillars, which are summarized as follows (Nieto, 2005). Pillar I (minimum capital requirement) seeks adequate risk management by banking institutions by promoting the development of proprietary (self-developed) risk management models. By comparing the probability of an event (loss) occurring with the cost that it would cause, it is possible to analyze how in every operation there is an expected loss that is included in the budgets. On the other hand, unexpected losses may occur that have to be financed through regulatory capital. Finally, there may be catastrophic losses that will have to be financed depending on the policy followed by the company in question that suffers these losses. Pillar II (supervisory review process) has the dual objective of increasing supervision by the Central Banks and at the same time making bank management more professional. Thus, companies must have a process for assessing the adequacy of their capital based on their risk profile, as well as a strategy for safeguarding their capital. In order to carry out this principle, tasks must be developed that include oversight by the board of directors,

capital and risk assessment, monitoring and reporting, as well as the review of internal controls. On the other hand, the supervisory authorities must examine and evaluate companies' internal strategies and assessments related to capital adequacy, as well as their ability to monitor and ensure compliance with regulatory capital ratios. In Pillar III (market discipline), the aim is to standardize the management of market information, ensuring its correctness and transparency. In this way, all the rules affecting the market where the economic activity is carried out, as well as its behavior, would be made known and understood.

Taking these pillars as a reference, it is already clear that the direct application of Basel II regulations is, at best, indirect and of little value for the scope and type of operational risks in a telecommunications company. However, Nieto (2005) makes an interesting contribution by describing the ten principles for risk management, administration and assessment (BCBS, 2003; BCBS 2004), since they show their validity for any company or organization. The only notable criticism would refer to their generality, their theoretical nature and difficulty of direct application. The principles are structured as follows. In the internal risk management unit, the first three principles refer to a company's internal risk management organization. In principle 1, the board of directors should be aware of the general principles of operational risk, as well as periodically review and approve the operational risk strategy. These actions shall include the definition of acceptable levels of risk and associated tolerances. In principle 2, managers shall be responsible for implementing the operational risk management strategy approved by the board of directors. They shall also be responsible for deploying operational risk management policies, processes and procedures throughout the company's value chain. In principle 3, information flows within the organization shall establish and maintain an effective working environment for operational risk management, facilitating management and the board of directors in their respective management and oversight functions). Regarding responsibility for operational risk management, four other principles, enunciated by the same document, indicate the company's responsibility for operational risk management. In principle 4, companies should identify the operational risk associated with all their products, services, processes and systems, seeking to minimize potential negative impacts). In principle 5, companies should establish the necessary processes for operational risk assessment. In principle 6, companies should have in place to monitor operational risk. In principle 7, companies should have policies, processes and procedures to control or mitigate operational risk in a manner consistent with their risk profile). As regards special roles in operational risk management, in Nieto's (2005) document, there is also a paragraph for market regulators (supervisors) that is

specifically addressed to public or private bank control and auditing bodies, which in the case of the proposed research project can be extended to telecommunications market control bodies (such as the Telecommunications Market Commission (CMT) [Comisión del Mercado de las Telecomunicaciones] in Spain), or to the competent bodies for the supervision of companies that, for example, are listed on the stock exchange and are accountable to their shareholders. For these supervisors, the set of principles to be applied is as follows. In principle 8, regulators should require companies to implement an effective system to manage operational risks. In principle 9, regulators should carry out regular and independent evaluations of operational risk strategies, policies, procedures and practices. They should also ensure that effective information and reporting mechanisms are in place. In principle 10, companies should provide sufficient information to stakeholders to ensure that their market participants can assess their exposure to operational risk. Crouhy and Mark (2006) study how to effectively implement an enterprise-wide risk management program, as well as indications in the financial sector about allocating capital and measuring performance, as well as contents on Basel II. The Basel III Accord, which includes BCBS (2011), was agreed in 2010; however, implementation is scheduled to be introduced in 2022. Nevertheless, it is not expected to include major changes in respect of the implications for the fundamentals and extrapolation of contents from the financial sector to the telecommunications sector discussed in this study.

Furthermore, as regards the measurement of operational risk, BCBS (2003; 2004) proposes AMA (Advanced Measurement Approach) as a more sophisticated method, where the capital requirement is determined according to the estimate of the operational risk to which the entity is actually exposed. To make this estimate, internal statistical measurement models are developed. This methodology for determining the capital requirement for operational risk using AMA models is similar to the concept of VAR (Value at Risk) used in this research. Based on the estimation of the aggregate loss distribution, the capital requirement required by Basel standards (BCBS 2003; 2004) is the one that aggregates 99.9% of the losses per year. Thus, the entity must demonstrate sufficient capital to absorb losses arising within one year in 99.9% of the cases, exposing itself to an insufficiency in the remaining 0.1% of the cases. In any case, AMA has been questioned even by experts in this field in the financial sector, not only because of methodological aspects related to the calculation models for extreme values and their correlation (Grody *et al.*, 2006), but also because of the problems involved in its practical implementation, for example due to the use of internal models that may be biased (Moosa, 2008). All this in the context of the financial sector, how much more so for the

telecommunications sector that is the subject of the research, where, moreover, there is no proven experience or studies. For this reason, and after its review, LDA (the Loss Distribution Approach) is proposed as an advanced measurement method, which is widely used as a model for quantifying operational risk (Klugman *et al.*, 2004). This approach was one of the first tools implemented by organizations to monitor their risk profile through a database of loss events (Breden, 2008). It has been widely used in the insurance industry and has become one of the most widely used tools in the banking environment. The objective of LDA is to obtain the aggregate distribution function of operational losses. This distribution is obtained from the accumulation of loss distributions for each line of business, for each type of risk or for a combination of both. Apart from the complexity associated with the conditions under which this LDA approach provides acceptable levels of accuracy (appropriate selection of frequency and intensity distributions, appropriate parameterization of the selected distributions, for example we agree with Breden (2008) when he argues that loss databases hardly provide information for loss events of low probability of occurrence and high impact, such as, in the case of a telecommunications company, e.g. a fire at a facility or the breakage of a highly protected submarine cable; even more so when such databases are almost non-existent, as is the business case of TELCO in this research). This argument, together with the complexity of building such a database, as discussed below, confirms that this will not be the preferred approach to undertake the investigation. In any case, it is true that the output parameters used in this technique may be valid in the formulation of the operational risk identification and evaluation model (i.e. aiming at being extrapolated to the telecommunications sector through this study). The phenomenon of operational losses can be disaggregated into two components: (i) the frequency (representing all possible amounts of events with their respective probability); and (ii) the severity or intensity (representing all possible loss values per event and their probability, once the event has occurred). For calculation purposes, both the frequency distribution and the severity distribution could eventually be estimated based on the operational losses observed by the entity and recorded in its operational loss database. In fact, the reasons put forward for not using such an approach are generally related to the high cost (in terms of money and time), but more importantly to the impracticality of being able to create and organize reliable and updated loss databases. Moreover, as Fraser and Simkins (2008) point out, it is often the case, especially for non-financial sectors, that once constructed they offer very limited value. This could be mitigated if it were possible to foresee that the risks to be quantified and managed would materialize with a considerably high frequency in the future, a fact that is quite uncertain in many cases. As argued by Breden (2008), this type of assessment based on event frequency and

impact is usually carried out on the basis of working sessions or workshops led and supported by the company's management, so as to ensure adequate dialogue for the efficient capture of data in an accurate, practical and realistic manner.

Pakhchanyan (2016) performed a complete survey of operational risk management literature for financial institutions which provides evidence of advanced techniques based on operational losses distributions for risk identification and evaluation for the financial sector. The author also develops the operational risk concepts following the Basel Accords where the foundations are the operational loss data. Financial risks being central to business, every financial institution is also exposed to multiple non-financial risks which tend to be hard to identify and evaluate, as in any firm. Thus, successful financial institutions have a sophisticated understanding for identifying and evaluating their core financial risks (primarily, credit and market risks); however, these companies also face operational risks exposures related to customers, information technology and processes, among others, defined as non-traditional risks in this financial sector. While non-traditional risks can have a real impact on the financial performance of an entity, they have been considered as incidental, and therefore denominated as non-financial risks. The professionals in the financial units tend to be experts in evaluating the activities that generate the financial risks, but they are less knowledgeable about the non-financial risks, including operational risks (Brown *et al.*, 2019). In fact, operational risk is not a new concept for financial institutions, as operational losses have been reflected in banks' balance sheets for many decades (Chernobai *et al.*, 2007). In summary, the concepts and philosophy underlying the aforementioned principles and the measurement of operational risk according to the Basel Accords will serve as the basis for the construction of the operational risk identification and evaluation model that is the general objective of this research.

A lesson learned from financial services organizations attributes considerable importance to benchmarking themselves against their peers only, instead of looking outside of their sector. Chew (2008), editor of the *Journal of Applied Corporate Finance*, makes a compilation of articles on risk management that provides a global view of risk management, especially for the financial sector. For this reason, in order to gain knowledge and experience for enhancing performance and results, it is reasonable to build ERM models for other sectors and consider a business case or case study approach (Ashby, 2008) which is the focus of this research. Therefore, it is recognized that despite these advances for the financial services, there should be relevant lessons to be learnt from other industry sectors such as manufacturing and energy production,

or from others where knowledge about risk management is scarce, such as in the telecommunications industry. One fundamental difference between the financial sector and other major industrial services is that financial factors, such as capital analysis, are better studied and modelled than risk management and evaluation in other industrial services where operational events and losses are the result of multiple interrelating operational causes and events.

Nevertheless, in every sector, financial and non-financial, loss prevention activities, such as risk identification and evaluation, are needed for the success of firms; however, literature review shows that most ERM studies for identifying and evaluating risks are focused on entities belonging to non-telecommunications sectors. Baxter *et al.* (2013) relied on the financial services industry to evaluate ERM operating performance; however, the samples of their studies were only limited to firms within financial and insurance sectors, which are not generalizable to other industries such as the telecommunications industry. Prior economic and finance literature differs from non-financial firms in concepts related to investment and regulation which have implications for implementing risk assessment techniques, where financial firms have been developing studies for financial leverage, profitability, and price setting behavior, while non-financial firms have not exploited this vast knowledge and research (Armstrong *et al.*, 2016). Furthermore, as studied by Breden (2008), operational risk evaluation for non-financial firms is not an easy practice for the following reasons: (i) operational risk is highly context-dependent: it is concerned with the risk of loss resulting from the failure of systems, processes, people, and from external events, and all firms have different processes, systems and practices to face them; (ii) there is no static portfolio of operational risks: the new challenges are showing up every day due to innovation and new technology (e.g., cyber risk); and (iii) there is no defined risk portfolio: while, for example, considering an individual credit risk it is easy to identify the amount of exposure, for an operational risk (e.g., fraud or systems failure) it is very difficult to evaluate how great a firm's exposure might be. Nevertheless, recent research for non-financial industry is gradually becoming more frequent as with the study developed by Ibrahim and Esa (2017) for the construction industry, where it can be found to be an interesting approach for data collection and analysis which led the authors to conclude that ERM implementation has positive significance to be applied in an organization to enhance the firm performance either in financial or non-financial aspects. Wieczorek-Kosmala (2014) reviews why and how risk management issues grow in importance within both financial and non-financial firms. The main reason for this trend is the rapid dynamics and constant hardening of business operations. An efficient implemented risk

management approach is helpful in overcoming obstacles and in providing organizations with a competitive advantage over those companies that do not manage risk. ERM frameworks are usually perceived as the procedures applicable for financial entities, due to the fact that in the financial sector the problem of excessive assumption of risk is the main concern where the regulatory bodies address the issue of capital adequacy, providing clear evaluation methods the financial institutions are expected to meet (BCBS, 2006). However, ERM and its associated methodologies should be implemented in any type of organization, regardless of its sector. A complete overview of relevant topics covered in this literature review is described by Chapman (2008), which includes a detailed explanation of ERM, the risk management process, as well as a good classification of risks.

Additionally, and following the literature review of reference papers, the research based on case studies and best practices on ERM has proven to be an efficient approach (Woods, 2009; Fraser *et al.*, 2014), not only for the risk management discipline but also for related subjects such as sustainability and CSR (corporate social responsibility) (Forcadell and Aracil, 2019). Sriyalatha and Fernando (2015) also base their research case studies on analyzing the behavior patterns in the adoption of risk management practices by the companies surveyed, as well as on moving into a convergence between theoretical practices and those adopted by the firms in a diversity of industry segments. Also, Tarantino (2006) had already developed insights regarding COSO, ERM, Basel II, as well as Sarbanes-Oxley, among other good governance frameworks, based on best practices and case studies; a case study approach to effective planning and response regarding operational risk management is provided by Abkowitz (2008)[9].

Within every national economy, the companies in the telecommunications sector stand out as a specific segment of the service sector characterized by increasing competitive challenges and exploration of new opportunities for generating innovative networks and services, which lead these companies to redefine their role in the market as well as to create new business models for new sources of profit, based on ERM frameworks and tools (Wu *et al.*, 2011). In fact, due to the type of services provided by large telecommunications services companies, very capital intensive and somehow intangible compared to other physical products, this makes it necessary for them to pay attention to ERM, from risk identification and risk evaluation to selection and implementation of

[9] More references on the advantages and need of the case study approach for this research are provided in sub-section 3.1.1 (methodology).

the appropriate risk management methodology. This is key for protecting the company's property and profit by decreasing potential losses. An interesting study for telecommunications business operations was developed by Dos Santos *et al.* (2005) where the concept of service level assessment is explained, which is a theoretical concept related to operational risk evaluation. Arena *et al.* (2010) used a case study of a wide range of telecommunications services providers to highlight the importance of using risk self-assessment and scenario analysis for helping organizations in linking risk management with business strategy and objective-setting for the business decision making process. Gandini *et al.* (2014) developed an empirical investigation on sustainable deployment for telecommunications companies, which depends on the ability to manage risks in a responsible way. Literature reveals that risks in the telecommunications domain are complex to evaluate due to lack of methodologies for predicting emerging threats to the services and this is costing telecommunication operators billions of dollars (Yesuf, 2017). One main reason for this loss may be that there is little emphasis given to the important steps of risk identification and evaluation within the risk management process, unlike other sectors where there is much more research and experience in risk assessment approaches. Foto *et al.* (2018) use a case study for risk management in the telecommunication industry. They reviewed the advantages and disadvantages of financial risk management in the telecommunications industry. The study included an assessment of financial risk management practices for the industry based on reliable data and statistical research. There are recent studies (Sehrawat, 2019) that examine the nature and strategies of risk management in large companies, such as Nokia, where general and theoretical patterns and drivers for risk management are described to ascertain how the company's strategy is managing risk. They describe the "what needs to be done" but leave for future research the "how to implement ERM", in particular the way to evaluate operational risks. Kozarevic and Besic (2015) describe the efficiency of existing procedures for risk management and the possibility for improving the existing situation in the telecommunications sector, using the methodology of case study for "BH Telecom" company. Their research develops the specificities of risk management in telecommunications services including a risk classification and a brief general description of methods based on the postulates on statistics and actuarial mathematics (through a theoretical model and questionnaires) for this sector, highlighting the importance of measures for loss reduction of perils and risks. They conclude that it is necessary to provide constant evaluation of a company's risks to understand their impact and probability of occurrence for every operational risk. In line with this, Dickstein and Flast (2009) had already developed a business process approach to managing operational risk.

Another capital intensive sector is electricity. Electricity companies (utilities), as public service providers where the continuity and quality of electricity supply are basic elements of their activity, should always pay special attention to operational risk in their activities through the use of various control and mitigation mechanisms for this type of risk. In this sense, the EURELECTRIC (2007) White Paper on role of electricity has studied that electric companies annually allocate a large amount of resources for the mitigation and management of their operational risks, through the development and acquisition of new assets, preventive and corrective maintenance measures, development of safety procedures and underwriting of insurance policies with increasingly comprehensive coverage.

A comparative analysis of operational risk exposure in the electricity industry in relation to the other risks (credit, financial, energy market and business) shows that operational risk is as important as any of the other types of risk mentioned, to which preferential attention has been given (in general, the energy industry has developed a notable number of risk models designed to control the price and volume risks of energy commodities or exchange and interest rates). These same conclusions are obtained in other markets, such as financial institutions, which have extensive and proven experience in operational risk measurement despite the fact that, theoretically, they could be thought to be less exposed to operational risks than a power company that is exposed to failures or accidents in its physical assets or to the interruption of electricity service. In line with the EUROELECTRIC (2007) paper I on risk management, there are several additional reasons that support the importance and benefits of operational risk management as a strategic fact: improved resource allocation, policy optimization, as well as those associated with corporate governance and regulatory compliance.

Based on the above, the beneficiaries of the operational risk model will be not only the risk control and internal audit functions of the companies, but also the managers of the different business units, as well as the company's management. According to the EURELECTRIC (2007) reports describing the need for ERM, the definition of ERM, the guidelines for ERM implementation, as well as the operational risk management approach, electricity companies have been focusing their operational risk management on exclusive control of accidents, failures and breakdowns of their generation or transmission and distribution assets, so that quantification is generally focused on the direct cost of repairing or replacing damaged equipment. Therefore, it does not consider, for example, the other operating costs that may be incurred in the entire value chain of the electricity network; nor does it consider other sources of operational risks, such as

losses caused by suppliers of equipment or services or losses arising from failures in the processes of operation of assets, external or internal fraud, regulatory non-compliance, among others.

In contrast to the aforementioned management method, experience in this sector reveals that some of the fundamental characteristics of operational risk are: (i) very diverse situations of operational events that may appear in different types of companies (generation, transmission, distribution, commercialization) and in the business units and activities thereof; (ii) capacity of propagation of the consequences of an operational failure that occurs in a given process, activity or business along the value chain of a company, in other words, an operational event can be the cause of a chain of operational events in a company; and (iii) difficulty in assessing the number of times an operational event can occur and the cost it can have, particularly if we consider the whole set of costs incurred as a result of the aforementioned propagation of the operational event along the company's value chain[10].

On the other hand, regarding the research design, the methodology and techniques of this study considers various concepts studied by Renn (2008) such as: (i) the definition of risk, which contains three elements: outcomes that have an impact, likelihood of occurrence, and the specific context in which the event may materialize; (ii) the scope of negative effects about the undesirable outcomes; (iii) the conceptualization of uncertainty for qualifying or quantifying (evaluating) the risks; and (iv) the rule of aggregation for practical conclusions of risk impact and probability of occurrence. Several authors support the use of actuarial analysis (Cohen, 1996), probabilistic risk assessment and scenario techniques (Bedford and Cooke, 2001) in an attempt to predict risk impacts and likelihood, and loss-probability functions for showing distributions of information gathered in the interviews with managers (Kolluru, 1995) and data aggregation through Monte Carlo simulations (Forester *et al.*, 2006). Operational risk quantification can be based on the extreme value theory (EVT) (Embrechts *et al.*, 1997) applied in the way that the tail of the operating loss distribution (the distribution of losses estimated for value-adding process using a statistical method) is fitted separately by fat-tail distributions, such as the Weibull distribution, whereas the empirical distribution is

[10] As reviewed in this research after analyzing the study for a company in the telecommunications sector (TELCO), there are important analogies between this and the electricity sector. However, no further details were found, other than those basic concepts mentioned, to base this research on techniques and tools for the identification and evaluation of operational risks in the electricity sector that could have been applicable to a company such as TELCO.

used for the lower part of the loss distribution. Additionally, Diebold *et al.* (2000) and Thomas and Pearson (2000) review and study the applicability of extreme value theory to risk management as well as the Value at Risk (the cumulative value of the operating losses at a specific confidence level and for a specific period) and threshold (the value of loss in the distribution that separates losses using the EVT) concepts. In accordance with Barton *et al.* (2012), ERM and risk evaluation cannot be stagnant, they should be organic and alive. To be consistent with this recommendation, the methodology considers a unique data set obtained from management through surveys and interviews, in order to estimate the variables for the loss distribution. The use of qualitative data to be collected and then quantitatively analyzed is becoming most natural in recent research (Saleem *et al.*, 2019), where the process of analysis is based on questionnaire distributions, resulting data to be expressed as statistical figures as well as to apply statistical tools needed to test the hypotheses or to build risk management methodologies. In fact, surveying through questionnaires the top/middle managers to obtain data related to operational risk evaluation is considered best practice (Beasley *et al.*, 2005). Damoran (2008) provides relevant content on risk assessment techniques and tools, including scenario analysis and Value at Risk approaches. Furthermore, one of the most useful approaches for establishing a framework for operational risk uses the technique of control self-assessment (Wade and Wynne, 1999). In this, a questionnaire or series of workshops are used to identify and evaluate relevant risks for the firm by asking the responsible parties within the company to subjectively assess various parts of the organization and its characteristics. In order to implement the control self-assessment (CSA) framework, the identification of events is needed for every business unit within the organization. Pickett (2005) develops phase by phase the control risk self-assessment tool. For each event category, specific questions are answered to gain insight into the associated risk and their severity and probability of occurrence. As explained by Jacobus (2015), control self-assessment, the basic element for a risk self-assessment (RSA) approach is at the core of ERM as a process and method to engage management and employees in identifying and evaluating risks; it also drives the growth of risk and control ownership among the employees. Finally, an important aspect is that the accuracy of risk evaluation methods depends on the soundness of the risk model and the availability of data. The appropriateness of those risk models, such as ERM, is inherently linked to data availability and the impact and probability of occurrence of events. Whatever methodology is chosen, the firm needs to understand the likelihood and potential impact of the risks that it faces (Breden, 2008). Furthermore, the accuracy of risk evaluation methods depends on the measurability of outcomes and understanding of effects (Muermann and Oktem, 2003).

Blanco-Mesa *et al.* (2019) conclude about the importance of ERM implementation in large companies, where control measures to be implemented for risk evaluation are key for the management team. The executives need to prioritize risk management efforts, including the use of methodology and tools for evaluating and treating the information to improve the process of decision-making in uncertain contexts. Furthermore, the lack of a clear understanding of the alignment between the firm ERM programs and the industry's ERM frameworks and the lack of vast literature, may limit the development and implementation of ERM, including operational risk identification and evaluation systems for financial and non-financial firms. Karanja (2016) explains the two main industry-sanctioned ERM models – COSO II and ISO 31000 (2009) – that firms refer to when implementing ERM approaches. These standards and frameworks are the essential references on which this research is based in terms of the methodological point of view. While there are documented cases of effective ERM implementations which are included in various studies such as the ones from Aabo *et al*. (2005), Fraser (2010), and Fraser *et al.* (2014), most firms struggle with complexities associated with applicable methods for risk identification and evaluation, particularly in the telecommunications sector. In fact, ISO/IEC 31010 (2019) standard, Fraser and Simkins (2016) and Quail (2012) describe various useful techniques for implementing ERM, such as ERM frameworks, organizational approaches, risk indicators and risk assessments to allocate capital for mitigating risks (Toneguzzo, 2010), with the scope, in most cases, of the financial sector.

2.3 Business and operational risks in the telecommunications sector

The purpose of this review is to have a current version of the main business and operational risks in the telecommunications sector, with the purpose of being able to contextualize the results of this research in what is really happening today in terms of risks associated with the industry of a company such as TELCO. Both risk categories (business and operational) should be understood in a broad sense, i.e. they include other risks such as strategic risks, financial risks, technological risks and compliance risks. This categorization depends in each case on the source reviewed. First, we have reviewed the risks explained by TELCO Group[11], IIA (The Institute of Internal Auditors) and the consulting firm Management Solutions. We then analyzed the information provided by the so-called Big Four auditing, accounting and business consulting firms: Deloitte, PwC, Ernst & Young, and KPMG.

[11] TELCO, the case study company for this research is one of the main subsidiaries (29% revenue) of TELCO Group, as described in sub-section 3.1.2.

The idea is not to be exhaustive in the analysis, but to have the highest quality information possible, both in terms of its content and the relevant sources from which it comes. Thus, although this study has been carried out over a longer and previous period of time, much of the information associated with risks is still current and has even evolved in terms of its impact and/or probability of occurrence, and the data provided here can help us to understand the impact that the risks are having, and therefore the importance of knowing them and motivating us to study them, and in any case, to activate the contingency plans that are in our hands, both at a personal, academic and professional level. In addition, part of the risks shown are reflected in TELCO case study of this research, especially in the part of the proposed model where these risks are identified.

2.3.1 TELCO Group, Institute of Internal Auditors and Management Solutions studies

Starting with TELCO Group, and based on its Annual Report (Telco Group, 2020), the risks involved in its businesses include:

- Changes in general economic, business or political conditions in the domestic or international markets in which TELCO Group operates that may affect its business, financial condition, results of operations, cash flows and/or the performance of its financial indicators, including as a result of the evolution of the COVID-19 pandemic, the uncertainties in Spain, the impact of Brexit, the worsening of the fiscal sustainability in some European countries or increasing trade tensions in certain parts of the world.
- Compliance with data privacy regulations and the impact of TELCO Group's inability to comply with any such regulations, including liability for any loss, transfer or inappropriate modification of customer data or general public data stored on its servers or transmitted through its networks.
- Exposure to currency exchange rates, interest rates or credit risk, including in relation to investments or in some of TELCO Group financial transactions.
- Existing or worsening conditions in the international financial markets.
- The impact of current, pending or future legislation and regulation in countries where TELCO Group operates, as well as any failure to renew or obtain the necessary licenses, authorizations and concessions to carry out its operations and the impact of limitations in spectrum capacity.
- Compliance with anti-corruption laws and regulations and economic sanctions programs and the impact of any breach of any such laws, regulations and programs.

- TELCO Group's inability to anticipate or adapt in a timely manner to changing customer demands and/or new ethical or social standards.
- Changes in TELCO Group's competitive position, including as a result of the evolution of competition and market consolidation in the markets where it operates, as well as the impact of any failure to comply with any antitrust regulations or any regulatory actions imposed by antitrust authorities.
- TELCO Group's inability to anticipate and adapt to the rapid technological changes that characterize the sector in which it operates, or to select the right investments to make.
- TELCO Group's dependence on suppliers and their failure to provide necessary equipment and services on a timely basis or otherwise meet TELCO Group's performance expectations.
- The impact of unanticipated network interruptions.
- The impact of cyber-threats and cyber-security actions.
- The impact of impairment charges on TELCO Group's goodwill, property, plant and equipment, intangible assets, deferred taxes or other assets as a result of changes in the regulatory, business, economic or political environment or other factors.
- The impact of a decrease in TELCO Group's liquidity or difficulties in its ability to finance itself.
- The outcome of pending or future litigation or other legal proceedings.
- TELCO Group's ability to complete any pending acquisition, divestment or other significant transaction as planned or with the expected outcome.

TELCO Group is affected by a series of risk factors that affect this company exclusively, as well as a series of external factors that are common to businesses in the same sector. The main risks faced by TELCO Group, which could affect its business, financial condition, results of operations and/or cash flows are grouped into four categories: (i) business; (ii) operational; (iii) financial; and (iv) legal and compliance. As analyzed in this research study, the classification of certain risks is defined by each company and according to the objective pursued, so that some risks, such as, for example, those associated with events related to suppliers, could be understood as business risk or operational risk. The important thing is the coherence and consistency when typifying the different risks, which is one of the objectives of the study in identifying them. TELCO Group's risks are set out as follows:

- Business risks:

- TELCO Group's competitive position in some markets could be affected by the evolution of competition and market consolidation.
- TELCO Group's strategy, which is focused on driving new digital business and providing data-based services, increases its exposure to risks and uncertainties arising from data privacy regulation.
- TELCO Group requires government concessions and licenses for the provision of a large part of its services and the use of spectrum, which is a scarce and costly resource.
- TELCO Group depends on its suppliers.
- TELCO Group operates in a sector characterized by rapid technological changes and it may not be able to anticipate or adapt to such changes or select the right investments to make.
- TELCO Group may not anticipate or adapt in a timely manner to changing customer demands and/or new ethical or social standards, which could adversely affect TELCO Group's business and reputation.

- Operational risks:
  - Information technology is key to TELCO Group's business and is subject to cybersecurity risks.
  - Unanticipated network interruptions can lead to quality loss or the interruption of the service.

- Financial risks:
  - Worsening of the economic and political environment could negatively affect TELCO Group's business.
  - Unexpected and uncertain events, such as the emergence of the COVID-19 (coronavirus) pandemic, significantly affect TELCO Group's operations.
  - TELCO Group has, and in the future could experience, impairment of goodwill, deferred tax assets or other assets.
  - TELCO Group faces risks relating to its levels of financial indebtedness, TELCO Group's ability to finance itself, and its ability to carry out its business plan.
  - TELCO Group's financial condition and results of operations may be adversely affected if it does not effectively manage its exposure to foreign currency exchange rates or interest rates.

- Legal and compliance risks:

- TELCO Group is party to lawsuits, antitrust, tax claims and other legal proceedings.
- TELCO Group is exposed to risks in relation to compliance with anti-corruption laws and regulations and economic sanctions programs.

The IIA (The Institute of Internal Auditors) report (IIA, 2020) "Risk Focus in 2021" provides interesting insights about the unprecedented circumstances of the global coronavirus pandemic (GCP), COVID-19, in the context of risk management. Being the biggest global risk event in recent memory, it has shaped the outlook for the coming years. Nevertheless, coronavirus itself is not a main risk. Rather than posing new threats, the novel COVID-19 has exacerbated existing risks, prioritizing them and pushing organizations to think about them from different perspectives or assign to them new levels of priority, within their business objectives. This comment is important to note when we review the risk classifications; COVID-19 impacts on every event and situation of the risk profile of the organizations.

IIA (2020) has identified the following top fifteen risks that organizations, in general and in order of importance, faced in 2021, which are very similar of those for 2020:

1. Cybersecurity and data security
2. Regulatory change and compliance
3. Digitalization, new technology and artificial intelligence (AI)
4. Financial, capital and liquidity risks
5. Human capital and talent management
6. Disasters and crisis response
7. Macroeconomic and geopolitical uncertainty
8. Supply chains, outsourcing and ‘nth’ party risk
9. Corporate governance and reporting
10. Communications, management and reputation
11. Corporate culture
12. Bribery, fraud and other financial crime
13. Climate change and environmental sustainability
14. Health and safety
15. Mergers and acquisitions

For these reasons, the ERM approach and well-established risk management and internal control systems are needed more than ever to ensure the ongoing operation of the organization.

Management Solutions (2019) has identified, in its "Risk and internal control report. Challenges in the TMT industry", the trending topics and action lines in the TMT (Telecommunications, Media and Technology) industry in terms of risk and internal control, which include the following categories: (i) strategy and governance; (ii) financial control; (iii) risk topics; (iv) ERM; (v) other emerging risks; and (vi) support tools. The following are the main risks included in the above categories that are closely related to the content of this research:

- Definition of corporate risk appetite and integration of risks in the business strategy (COSO II update)
- Review of risk models, policies and procedures
- Technological risks and cybersecurity (e.g. information leakage; identification and securitization of critical assets)
- Evaluation of outsourcing and vendor risk management models
- Fraud prevention
- Evolution of the Human Resources Control Framework
- Implementation of whistleblower channels
- Development of risk maps
- Quantification of the control environment and linkage to risk management
- Quantitative development of risk assessment and integration into management
- Data and model risk management
- Reputational risk monitoring
- Development and measurement of climate and sustainability risk models

Within the global business context, telecommunications operators face different types of challenges that condition the achievement of their objectives. In this regard, Management Solutions (2019) analyzed the following top 15 challenges in terms of risk, arranged thematically by category: strategy, organization and culture, finance, compliance, and operations and technology:

- Strategy
    - Complex macroeconomic context and competition
    - Reputation and brand
    - Disruption and new technologies
    - Digital transformation
    - Sustainability and climate risks

- Organization and culture
  - Simplification of organizational structures
  - Talent management and corporate culture

- Finance
  - High investment barriers
  - Low returns and increased debt

- Compliance
  - Regulatory and administrative requirements
  - Privacy and security

- Operations and technology
  - Reinventing the customer relationship model
  - High dependence on suppliers
  - Failure of technology infrastructure
  - Data and models governance

2.3.2 The Big Four: Deloitte, PwC, Ernst & Young, KPMG studies

The following is a review of recent top risk analyses by the Big Four accounting firms, in order of their ranking by revenue in 2020: Deloitte ($47,600 million), PwC ($43,000 million), Ernst & Young ($37,200 million), and KPMG ($29,220 million).

Deloitte (2020), in the review study about refocusing risk and resiliency, analyzed how in 2020, risk management at financial and non-financial institutions faced challenges of a scale and scope not seen before as the world responded to the GCP (global coronavirus pandemic), also named GHC (global health crisis) caused by COVID-19. The measures taken by governments, organizations, and customers to restrain the spread of the COVID-19 triggered a sharp economic downturn and wide-ranging social impacts. COVID-19 has also had direct financial impacts on financial institutions and there is greater potential for fraud, such as from misuse of customer data. Unfortunately, and mainly for financial institutions, the pressure on revenues is likely to intensify the drive at many firms to reduce ever-increasing expenditures on risk management. Several key risk management trends emerge from the Deloitte (2020) analysis:

- Increasing credit risk, credit risk measurement being a very high priority for firms
- Greater focus on non-financial risks, where many firms and institutions have work to do to enhance their capabilities in this area

- Continuing concerns over cybersecurity, as organizations have to face more cyberattacks than ever, mainly for employees working at home
- Addressing risk from third parties where relationships present various risks such as data privacy, underperformance and unethical conduct
- Spotlight on environment, social, and governance risk, with high concern over climate risk and increasing attention on corporate social responsibility issues
- The potential of digital technologies to reduce risk management expenses
- Substantial challenges of risk data management, especially for non-financial risks due to various issues including maintaining reliable data to quantify non-financial risk and drive risk-based decisions
- Continued progress on risk governance, as the board of directors committees are responsible for risk oversight, supported by risk management experts, which is a sign of progress in effective governance
- Organizing a chief risk officer (CRO) position with appropriate authority to effect change regarding risk management and its impact in business operations

In summary, and according to the study conducted by Deloitte (2020), risk management functions will need the ability, flexibility and expertise to respond appropriately to volatile economic conditions and changing work practices.

PwC (2015) has been publishing a risk radar until 2015, an 'early warning system' which manages a broad spectrum of risks, financial, regulatory, compliance and reputational. Recently, PwC (2021) has been working on a draft version of the radar (not intended to be published) including 28 new/increasing risks (**++**), lineal trend risks (**+**) and decreasing risks (**-**), arranged into eight categories: (i) strategy; (ii) people and organization; (iii) customer; (iv) infrastructure; (v) operations; (vi) technology; and (vii) finance; and (viii) regulation and compliance; as well as two "global risks" impacting all categories, sustainability and COVID-19. The risks are the following:

- Strategy
  - Competitors and changes in competitive landscape (**+**)
  - Mergers and acquisitions (**++**)
  - Expansion and product development (**+**)

- People and organization
  - Talent attraction and people (**++**)
  - Climate change and social responsibility (**+**)
  - International mobility (**-**)

- Operating model and governance (**++**)
- Staff retirement benefits (**-**)

- Customer
  - Customer profitability (**+**)
  - Customer services and market communication (**+**)

- Infrastructure
  - Network maintenance (**+**)
  - Network planning, security and performance (**+**)
  - Technological advancement (**+**)

- Operations
  - Cost transformation and supply chain – Dependency of suppliers (**++**)
  - Third-party service providers and shared services center (**+**)
  - Business continuity management (**+**)

- Technology
  - Cybersecurity attacks and data protection (**+**)
  - Digital disruption (**++**)

- Finance
  - Revenue accounting standard (+)
  - Asset impairment (**++**)
  - Credit and investor relations (**+**)

- Regulation and compliance
  - Service quality (**+**)
  - Universal service obligation (**+**)
  - Billing accuracy (**++**)
  - Assets retirement (**+**)
  - Health and safety (**++**)

- Sustainability (**++**)
- COVID-19 (**++**)

The Ernst & Young (EY) (2020) report "Top 10 risks in telecommunications 2020" is part of an ongoing series of reports designed to highlight the most critical risks facing the telecommunications sector. The EY risk radar structures risk factors into four categories:

(i) strategic threats related to customers, competitors and investors; (ii) financial threats that stem from volatility in markets, ecosystems and investments; (iii) operational threats that impact the processes, systems, people and the overall value chain of the business; and (iv) compliance threats that originate in politics, regulations or corporate governance. The drivers of the risk universe, which reflect changing external factors, industry challenges and organizational priorities, are:

- COVID-19 has significantly impacted the sector, negatively affecting financial and network resilience in the near term while also prompting greater government and regulatory intervention.
- Geopolitical issues have a significant impact on the sector. Populism and economic nationalism are facilitating protectionism. 5G is core for an emerging technology “cold war”.
- Digital transformation initiatives are expanding telecommunications companies. Sustainability has a major focus at management and board levels.
- The telecommunications industry is undergoing far-reaching network modernization in both fixed and mobile segments.

The top 10 risks (Ernst & Young, 2020), organized according to the above categories are:

1. Failure to optimize infrastructure resilience and reach (core risk shared by all categories): “networks generally performed well during the COVID-19 crisis 2020”; there are sustaining positive customer perceptions” (e.g. telecommunication companies are experiencing materially higher network demand)
2. Inability to scale internal digitization initiatives (operational): “moving from digital-first to digital throughout is becoming critical as sustainable solutions become more important” (e.g. COVID-19 is forcing telecommunication companies to rethink their transformation plans)
3. Failure to redesign workforce purpose and inclusion (operational): “talent attraction and workforce diversity are top-of-mind issues in the sector” (e.g. talent acquisition needs are pronounced in domains such as automation, artificial intelligence and software-based networks”
4. Failure to improve capex efficiency and network returns (financial): “ensuring better outcomes from network investment is critical” (e.g. COVID-19 is prompting a greater focus on network reach and accessibility)

5. Underestimating changing imperatives in privacy, security and trust (compliance): “security remains a compliance-driven concern at a time when customer anxieties are mounting” (e.g. privacy and security concerns among customers are rising)
6. Poor management of investor and stakeholder expectations (financial): “COVID-19 has disrupted forward-looking guidance as operators exercise caution” (e.g. a number of telecommunications companies have withdrawn their full year guidance for 2020)
7. Ineffective engagement with industry verticals and public sector (strategic): “telecommunication companies have a greater role than ever to play across sector boundaries” (e.g. companies require greater support in 5G and IoT (Internet of Things))
8. Inability to adapt to a changing regulatory landscape (compliance): COVID-19 is affecting regulatory predictability as policy-makers shift their focus” (e.g. COVID-19 is prompting regulatory priorities)
9. Failure to mitigate evolving disruptive scenarios (strategic): “network supply chains are in flux while technology companies are taking new value chain positions in telecoms” (e.g. network equipment supply is subject to geopolitical and global trade forces)
10. Failure to take advantage of changing market structures (operational and strategic): “new whole sale opportunities are arising while infrastructure spin-off and switch-off remain in focus” (e.g. tower sale and leaseback, and infrastructure joint ventures continue to gain prominence worldwide)

Below the radar, EY (2020) includes the following risks:

- Lack of fit-for-purpose performance and sustainability metrics
- Ineffective digital growth and diversification strategy
- Disruption of supply chains
- Limited internal understanding of emerging technologies
- Ineffective capital allocation to drive value creation

The KPMG (2020) report “CEO outlook 2020”, and due to the COVID-19 pandemic, is putting existing risks in a new light and forcing organizations to think about them differently, in the following way: (i) talent and a new working reality (remote working and new ways of working); (ii) shifting risk agenda (‘talent risk’ has risen to be named as the most significant threat to the growth of their businesses ahead of ‘supply chain risk’); and

(iii) digital acceleration (mainly due to the lockdown). KPMG's top 15 risks, in order of importance, are the following:

1. Competition and market consolidation
2. Data privacy
3. Concessions, licenses and spectrum
4. Technological changes
5. Changing customer demands and/or development of new ethical and social standards
6. Dependence on supplier network
7. Cybersecurity
8. Network failures and service interruption
9. Deteriorating economic and political environment
10. COVID-19 pandemic
11. Asset write-offs
12. Level of financial indebtedness and financing capacity of the company
13. Exchange rates or interest rates
14. Litigation, tax, antitrust, competition and other legal proceedings
15. Anti-corruption compliance

2.4 Theoretical conclusions

The theoretical foundation has been structured in three basic areas: fundamentals of risk management, previous studies on identification and evaluation of operational risks, as well as business and operational risks in the telecommunications sector (2020). Based on this and on the research objectives (main purpose and research questions), we derive some research propositions, as described in section 2.5.

Regarding the fundamentals of risk management, a review has been carried out regarding the evolution of the risk management discipline, analyzing its impact and its basic definitions associated with the concept of risk and risk management. It is important to highlight the concept of risk as a business opportunity and the need to create a common language to undertake the central propositions of this research. This common ground becomes necessary because the interrelation with managers is essential to develop the case study of TELCO, the chosen telecommunications company.

In addition, the main risk management frameworks, standards and associated commissions were reviewed. This analysis has allowed the generality of these theoretical models to be corroborated while revealing the importance given to the steps in the

identification and evaluation of risks, COSO II, together with some techniques derived from the ISO 31000 standard. These constitute a good theoretical starting point for the development of the empirical research.

A literature review was then carried out in the hope of finding a solid model on which to base the research; in this sense, the lack of studies applicable to companies in the telecommunications sector for the identification and evaluation of their operational risks became evident. However, it was possible to explore the advances in financial firms, with great experience and knowledge in these matters, which inspired the formulation of the proposed research model, as will be seen below, through the extrapolation of certain quantitative and qualitative techniques. Specifically, Basel II has been a source of inspiration to develop the model, bearing in mind that its application is only focused on the banking sector.

Finally, despite being outside the temporal scope of this research, the main current risks have been reviewed, as of the date of recently published reports and referring to the year 2020. This review gives a sense of timeliness to the research, including the current pandemic crisis global risk. It also provides insights in key risks from the Big Four companies that permanently run radars for their detection, identification and assessment.

In short, the most important conclusions derived from the theoretical foundation are the following:

- The technological transfer characteristic described in the scientific contribution is fulfilled, i.e., the knowledge transfer in the risk management discipline (researchers, practitioners, managers, scholars, among others).
- The importance and treatment that other studies, frameworks and standards give to the steps of risk identification and assessment are identified.
- It has been identified that the standards, frameworks and models reviewed do not meet the objectives of this research, hence the need of this study. This is particularly relevant in the case of a telecommunications company where the theoretical and literature review reveals the following: (i) existence of robust operational risk assessment models in the financial sector; (ii) lack of studies of operational risk management models in the telecommunications sector; and (iii) complexity of standards and frameworks to be implemented in a firm with an understandable and practical (not so theoretical) approach.

- To formulate a risk identification and evaluation model, a lean, useful and applicable process is required. The risk management processes reviewed in both ISO standards and COSO frameworks provide processes that are too theoretical and complex to be applied to a company such as TELCO, or any other company in its sector or even in another industry where there are large and complex firms. Therefore, a framework to a risk management process has been developed based on fundamentals of risk management and literature review.
- Finally, based on the theoretical foundation review, we include in section 2.5 the **research propositions** aligned with the main purpose and research questions of this study, based on the research objectives and the theoretical conclusions.

2.5 Research propositions

Once the basic contents of the theoretical foundation have been studied and considering the main purpose, the research questions and the objectives formulated in this research, we briefly proceed to include two specific propositions[12]. These propositions will be analyzed in empirical study and the results will show the extent to which the evidence of the case study and the models created supports them. Both propositions are based on the two steps (identification and evaluation) of the risk management process described in section 2.1.3.

Based on the main purpose, which is the possibility of creating and applying an operational risk identification and evaluation model for a company in the telecommunications sector, the specific research **propositions** are:

1. It is possible to create frameworks for identifying the operational risks of a telecommunications company for a large firm in this sector.
2. It is possible to develop an assessment methodology and apply it for evaluating the operational risks of a telecommunications company for a large firm in this sector.

[12] The terms "proposition" and "hypothesis" both refer to the formulation of a possible answer to a specific scientific question. The main difference between the two is that a hypothesis must be testable and measurable, while a proposition deals with pure concepts for which no laboratory test is currently available. A proposition is a statement about a concept, either naturally occurring or constructed, which is the case of this study.

3. EMPIRICAL STUDY

The empirical study of this research is based on the theoretical contributions studied, and should contribute to the fulfillment of the research objectives. The theoretical foundation, despite showing that there is not much literature for the development of research in the telecommunications sector, has identified risk identification and evaluation techniques applied in financial institutions that can be extrapolated to other sectors (particularly in the measurement of risk based on loss distributions, VaR, actuarial techniques and simulations and convolutions via Monte Carlo). In this sense, previous studies on operational risk identification and evaluation, as indicated above, have made it possible to dismiss certain approaches that are not applicable to non-financial sectors, but have also contributed concepts and working lines that are used in this empirical study. In addition, concepts analyzed in this literature, such as self-assessment, provide information and knowledge for the development of the operational risk identification and assessment model under study. In relation to frameworks and standards, ISO/IEC 31010 is an important contribution to the assessment techniques used. Also, the review of risk management processes based on ISO 31000 and COSO standards has allowed them to be known and simplified. Also, an effective risk management process framework is basic for the empirical study to describe the steps of risk identification and evaluation, and its application to TELCO. Furthermore, creating a common language and a certain "culture of knowledge" on risks through the review of risk management fundamentals is key for the development of the empirical study.

On the other hand, the operational risks identified in the updated studies of the recognized sources consulted, especially those of the Big Four, will make it possible to contrast the existence and priority of the risks already analyzed at the date of the study, a very convenient exercise to check the robustness of the proposed model with a view to incorporating or disregarding operational risks in successive applications of the model. Finally, the conclusions in this section should corroborate, contrast and analyze the specific propositions.

3.1 Research design

Yin (1994) identified five components of research design that are appropriate for case studies: (i) research questions; (ii) propositions; (iii) units of analysis; (iv) the logic for linking the data to the propositions; and (v) the criteria for interpreting the findings. All of them are included in this research. Research questions as well as the main purpose are described in sub-section 1.1 (research objectives). Specific propositions are stated in

sub-section 2.5. Units of analysis are included in sub-section 3.1.2. And the logic for linking the data to the propositions and the criteria for interpreting the findings are analyzed in sub-sections 3.2 (operational risk identification and evaluation model), 3.3 (analysis of results), 3.4 (empirical study conclusions) and 4.1 (main findings).

3.1.1 Methodology

In order to understand the methodology of this research, we considered the following contents: (i) case study approach; (ii) research scope; and (iii) risk assessment techniques and data gathering.

3.1.1.1 Case study approach

The main objective of this study is precisely focused on creating, describing and applying an operational risk identification and evaluation model based on two pillars: the operational risk identification frameworks and the operational risk assessment methodology (RAM). The RAM integrates two interrelated components: an operational risk self-assessment process (OpRSA process) and an operational risk self-assessment method (OpRSA method). Both pillars will be built, illustrated and analyzed using a case study approach (e.g., Ashby, 2008; Ching and Colombo, 2015; Forcadell and Aracil, 2019; Foto *et al.*, 2018; Fraser *et al.*, 2014; Woods, 2009), applied to a specific global telecommunications company (TELCO) from TELCO Group. TELCO company case study, as it is described in the analysis of results, is aligned with the primary purpose described in the research objectives to create and apply an operational risk identification and evaluation model for a company in the telecommunications sector.

Considering that case study research is indicated when: (i) the study asks how and why something happens; (ii) the context is a relevant source of information; and (iii) the conditions in which the activity is performed are not able to be controlled (Patton and Appelbaum, 2003), we used the case study methodology (Yin, 1994), considering a real company (TELCO) approach to identify and evaluate its operational risks. Furthermore, this approach is recommended when there is a need to understand the decision making and the actions to construct models when changes in business processes are occurring (Siggelkow, 2007). Also, due to the fact that the existing literature of risk identification and assessment for telecommunications companies is scarce, a case study technique is suitable to further explore how the enterprises in the telecommunications sector address the implementation of a risk management model. In fact, the use of case study method has been successfully implemented to understand the contingency variables for risk

control systems in public sector organizations (Woods, 2009) as well as to investigate risk identification and evaluation maps (Jordan *et al.*, 2013), while surveys have also been an appropriate tool for risk management impact on organizational structures in the banking industry (Wahlström, 2009). All of these reasons legitimate the use of the case study methodology for a company such as TELCO.

3.1.1.2 Research scope

The methodology for defining the scope of the risk identification and evaluation pillars in TELCO was analyzed. It can follow two different approaches depending on the desired level of detail within TELCO's organizational structure:

- Bottom-up vs. Top-down (different levels of investigation according to the information required and to the level of detail of the questions and answers in the data gathering process).
- Whole vs. Partial (different scopes of implementation, i.e. entire company vs. specific and relevant units of the company).

Table 3.1 depicts the advantages and disadvantages of choosing the different scopes for TELCO.

Table 3.1. Field Work Scope Approach

SCOPE	Bottom-up vs.Top-down		Partial vs. Integral	
PROS	-More precise risk identification and measurement -Better knowledge of risks -More specific identification of risk factors and mitigating actions	-Quick to implement -Lower impact on organization (in terms of units involved) -Attainment of risk information with adequate level of detail for top management	-Possible fine tuning of the OpRSA method -Results very specific and detailed	-Immediate understanding of the risk profile of the company -Immediate use of the results for the calculation of the overall Capital at Risk
CONS	-Implementation is more complex, requires more time and has a high impact on the organization	-Measurement might be less precise -Risks investigated are more generic and consequently risk factors and mitigating actions	-Limited in the scope of the application of the model (units chosen must be relevant)	-More difficult to implement

For both the risk identification and risk evaluation pillars, the scope we decided for TELCO was the top-down and partial approach. We made this decision based on managers' commitment in their roles as interviewees, the number of business and support units involved for identifying the events of TELCO (eight, in total), and two business units (Fixed Line and Mobile Line) for applying the risk assessment methodology, as well as for the following reasons:

- Less impact on the organization. It was considered that the analysis based of new concepts entailed by the study of a new operational risk identification and evaluation model, more complex than the know-how on risk matters that TELCO had evolved before this study, advised a partial and top-down scope for facilitating the study and the progressive learning process needed by the organization.
- Quick implementation. In an organization of TELCO's size, a top-down approach leads to achieve results of the study in a faster way.
- Optimization of the operational risk management methodology. This approach allowed the research to be done in a way to practically gauge whatever adjustment was needed for the questionnaires and parameters for the operational risk self-assessment method and the OpRisk SW system described in this study, in the identification of events and in their evaluation.
- Greater effectiveness in the rollout phase of the operational risk assessment methodology, in case TELCO ever decides to extend this study to a greater scope for all its business and support units, and not only for the Fixed Line and Mobile Line business units.

3.1.1.3 Risk assessment techniques and data gathering

The fundamental references for defining the methodological aspects of this study are included in ISO 31010 (2009) and ISO/IEC 31010 (2019) international standards, which develop and suggest the main risk identification and risk evaluation techniques, classified under the risk assessment component of the ISO 31000 process (ISO 31000, 2018), previously reviewed in section 2.1 (fundamentals of risk management). Also, the operational risk assessment methodology development was based on the use of data collection analysis (Saleem et al., 2019; Ibrahim and Esa, 2017), through questionnaires (Beasley et al., 2005) responded to by managers of TELCO, statistical techniques on operational loss distributions (Pakhchanyan, 2016), risk assessment tools (ISO/IEC 31010, 2009), as well as the application of control and risk self-assessment approaches (Jacobus, 2015; Wade and Wynne, 1999), actuarial analysis (Cohen, 1996), probabilistic risk assessment and scenario techniques (Bedford and Cooke, 2001), Basel II recommendations (BCBS, 2006), as well as the COSO and ISO 31000 frameworks (Karanja, 2016), among other referenced theories included in this study. Supporting information was also used for the methodology, from sources such as Quail (2012), who describes risk workshops and interview development that involve brainstorming to facilitate data gathering for risk identification and management across the firm, and

Fraser (2010), who presents relevant information which was a reference for conducting risk working meetings and interviews.

For the risk identification pillar, managers from four core business units and four support units of TELCO were involved (as shown in sub-section 3.1.2, TELCO company analyzed). Based on the identification of TELCO's operational events, risk factors and risk effects, we used primary data (topics addressed at workshops and interviews), supported by eight questionnaires and secondary data (key TELCO internal information owned and used by the managers) (Eisenhardt, 1998). We conducted four workshops with TELCO's core business units, which lasted an average of four hours each, and four in-depth interviews with TELCO support units' managers, which lasted in total an average of two hours each. In both cases, brainstorming sessions following semi-structured questions were useful tools.

For the risk evaluation pillar, managers from the Fixed Line and Mobile Line business units, which are the ones under the scope of this research for assessment, were involved, specifically, the six segments or organizational units analyzed in the Fixed Line business unit and the five segments or organizational areas included in the Mobile Line business unit (see sub-section 3.1.2). By interviewing knowledgeable managers who were responsible for operational risks in the two relevant business units under the scope of the study, we accomplished the purposive sampling requirements of competence and experience (Hughes and Preski, 1997; Payne and Mansfield, 1973). We ran 11 questionnaires, one for every segment or organizational unit, supported by semi-structured workshops, following ISO 31010 (2009, 2019) guidelines, which were approximately six hours long and were staggered across eight weeks, allowing the researcher to improve the questionnaires by incorporating additional secondary data into the design of the interview check-list based on the insights suggested by the interviewed managers as key informants (Yin, 2009) and enabling reporting of rich contents as follow-ups with the managers clarified issues that were discussed in earlier interviews (Kvale, 1996). We also conducted two in-depth interviews with the managers of both core business units. As is common in all case studies, in order to avoid biased answers, we triangulated our emerging themes and findings (Eisenhardt and Brown, 1998; Perry, 2001) in the interviews with secondary sources of data coming from various managers and external audit reports with interest in the same event of risk. The information obtained and supported by the in-company software, OpRisk, sheds light on the inputs requirements (estimated frequency, estimated severity and estimated worst case impact) turning it into the outputs (losses distributions and risk classes). Not much data could be

examined as secondary information, with the exception of the abovementioned in-company information and some light reference to risks in an overall approach, given that this is the first time that this study has been developed. Furthermore, for the risk operational risk assessment methodology, on the basis of an operational risk self-assessment process and method, the control risk self-assessment (CSA) approach has been used. In fact, as explained by Pickett (2005), CSA is a powerful tool to support risk management frameworks, and is about getting managers and the work team to self-assess information about risk, typically in workshops and facilitated meetings, which is the case with TELCO. For the identification and evaluation pillars, and prior to the workshops and to gain cooperation (Lynn *et al.*, 1998), we sent the interviewees an interviewer's guide (see Appendix A, which includes the theoretical rationale and illustrations of reports generated by the OpRisk SW including not only the questions, but also specific and aggregated information of the study results) including the questions to be answered throughout the sessions with the main questions to be discussed.

To summarize, the research technical data sheet is described in Table 3.2:

Table 3.2. Research Technical Data Sheet

Sector	Telecommunications
Business case	TELCO Company (subsidiary of TELCO Group with presence in Europe and Latin America)
Company main figures	30,000 employees; 12,000+ million euros revenues, 5000 million euros OIBDA, 41+ million accesses (customers)
Units for analysis (risk identification)	Business and support business units (8)
Units for analysis (risk evaluation)	Fixed line and mobile line business units
Methodology	Case study
Research scope	Top-down and partial
Period of analysis and date of completion	September 2016-July 2021. Some TELCO´s data available prior to 2016.
Information sources	TELCO Group Annual Report (2020) and information, TELCO OpRSA SW, field work with TELCO´s managers, theoretical foundation contents

3.1.2 TELCO company analyzed

As stated in the 2020 Annual Report (Telco Group, 2020) of the company, TELCO Group is "a telecommunications service provider with its footprint in some markets in Europe and Latin America. Its objective is to create, protect and promote fixed and mobile connections for customers helping them to take control over their digital lifestyle. Therefore, TELCO Group primarily offers its customers the connectivity they need to interact and live in the markets where the company operates through simple products and services while protecting their data and managing it in a responsible way. TELCO Group relies on modern technology to create a better and more inclusive society. The company aims at offering its customers the possibility to reach the digital world

regardless of their location, economic status, level of digital knowledge and capacities*"*. TELCO Group's strategy aims to enhance value through: (i) making our world more human, by connecting lives in a sustainable way; (ii) offering good connectivity, which is the enabler for all digital services, by providing a wide range of services over connectivity through a fixed and mobile bundled offer; and (iii) focusing on customers' needs. In order to fulfill the previous objectives, TELCO Group has the following enablers: (i) end-to-end digitalization; the continuous effort towards this goal has resulted in a key lever in the COVID-19 crisis, by providing a rapid response to companies as they adapted to and sought to enhance their competitiveness in the new landscape; (ii) Big Data and innovation to add value to its customers; (iii) focus on the simplification of processes; this includes keeping a tight control over investments, supporting operating cash flow through cost savings and adapting to the new COVID-19 environment; (iv) digital trust, developing tools to protect information in end-user devices and communications, fixed and mobile, networks, as well as to protect customers' digital identity; this strategy is key in the new COVID-19 environment; and (v) fiber, 4G and 5G networks to continue to maintain high quality services for home offices and a higher consumption of entertainment services, and to drive the digitalization of companies, SMEs, and Public Administrations as well as individuals.

In summary, TELCO Group is a diversified telecommunications enterprise which provides a comprehensive range of services through one of the world's largest and most modern telecommunications networks, being focused on providing telecommunications services. It is one of the largest telephone operators and mobile network providers in the world. It provides fixed and mobile telephony, broadband and subscription television, operating in Europe and in Latin America, operating in 13 countries and with presence in 24, with an average of 113,000 employees, revenues of 43,000+ million euros, and 345+ million accesses (customers and others such as fiber-optic cables and smartphones) in 2020. TELCO Group is a global 100% telecommunications listed company in several of the most important stock markets around the world, including New York SEC, which is the United States of America Securities and Exchange Commission, with more than 1.3 million shareholders.

3.1.2.1 TELCO Group 2020 COVID-19 highlights

As reported in TELCO's Form 20-F to the United States Securities and Exchange Commission on February 25, 2021, for the fiscal year 2020, and its Annual Report (2020), "the COVID-19 pandemic affected TELCO Group throughout the year 2020, as lockdowns imposed across the firm's markets put unprecedented pressure on both its

B2C (Business to Customers) and B2B (Business to Business) segments. TELCO Group's estimates of the impact of the COVID-19 pandemic on the company's results were calculated on the basis of the difference between actual results and the results that they estimated would have been obtained if trends prevailing prior to the pandemic had not been interrupted. These estimates were made by TELCO Group in respect of those items that were considered to be most affected by the COVID-19 pandemic, namely, revenues (in particular, service revenues, roaming revenues and handset sales) and expenses (in particular, direct and commercial costs, supplies (including handset costs and bad debt costs), as a result mainly of the interruption of the commercial channel, international travelling restrictions, the temporary closing of some businesses and SMEs (Small and Medium Enterprises) in some regional subsidiaries and, more generally, depressed economic conditions. In order to support communities in which the company operates, TELCO Group implemented measures aimed at: (i) protecting the health and safety of its employees and customers; (ii) providing critical infrastructure and technology services to governments and health authorities; (iii) donating goods and services to hospitals and vulnerable customers; (iv) providing customers with free mobile data and additional entertainment services at no extra cost; and (v) accelerating payments to suppliers with liquidity problems and offering flexible payment terms to customers, among other initiatives. More importantly, TELCO Group's state-of-the-art networks have enabled the company to facilitate record growth in traffic driven by remote work and increased consumption of entertainment services while maintaining high levels of customer experience and service quality. Digitalization has proved to be a key lever for TELCO Group in this crisis, as processes were accelerating, needs were crystallizing, and the company helped communities and companies to adapt and to enhance their competitiveness in the new environment. Digitalization has emerged as one of the drivers of economic recovery. In 2020, TELCO Group continued capturing and retaining high-value customers focusing on customer experiences and the strength of its infrastructure…".

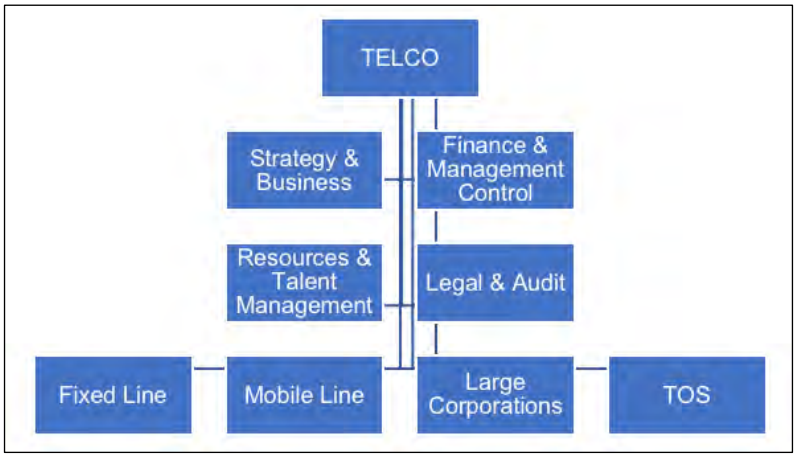
3.1.2.2 TELCO main figures and business units

The scope of the field work of this research is focused in one region (local country), the subsidiary named TELCO. The research started in 2016 with the understanding of TELCO Group, its operations, with the definition of the research objectives, as well as with the selection of TELCO as the company to be included in this study. Consistent data started to be collected from 2016 though previous data from TELCO was available since 2012 and before while the processing of the information to fulfil the objectives of the

research, in accordance with the methodology was between 2016 and 2018, before the COVID-19 pandemic occurred. The main figures of TELCO along the development of the research were aligned and did not change significantly in comparison with the current reported main figures in 2020 which are: an average of 30,000 employees, revenues of 12,000+ million euros, and 41+ million accesses (customers and connections through different technologies, handsets, computers, tablets, …), and OIBDA[13] of 5000+ million.

The organization of TELCO for the purpose of this study (four core business units: Fixed Line, Mobile Line, Large Corporations and Technology, Operations & Systems (TOS); and four supporting units: Strategy & Business Development, Finance & Management Control, Resources & Talent Management, and Legal & Audit), also mentioned in sub-section 3.1.1 (methodology) is depicted in Figure 3.1.

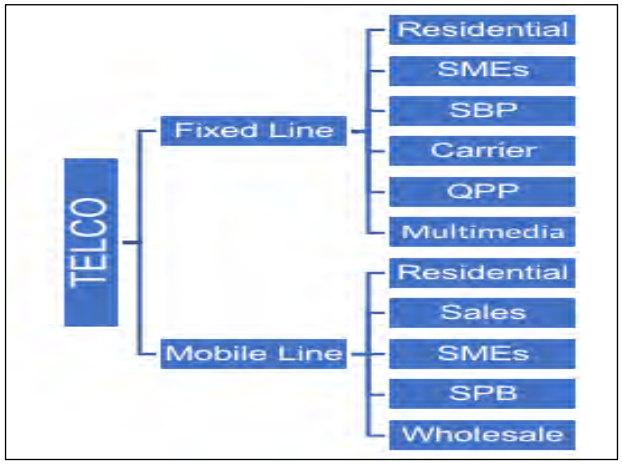
Figure 3.1. TELCO's Business Units. Source: TELCO's information



These functions were used in the operational risk identification pillar, while the study under scope for the operational risk evaluation pillar is shown in Figure 3.2. It includes: six segments or organizational units analyzed in the Fixed Line business unit: Residential; SMEs-Small and Medium Enterprises, Businesses and Professionals (SBP); Carrier Services; Quality, Products and Processes (QPP) and Multimedia. And five segments or organizational areas analyzed in the Mobile Line business unit: Residential; Sales; SMEs-Small and Medium Enterprises, Businesses and Professionals (SBP) and Wholesale Business.

[13] OIBDA (Operative Income Before Depreciations and Amortizations).

Figure 3.2. TELCO's Fixed Line and Mobile Line Business Units. Source: TELCO's information



3.1.2.3 TELCO products and services

Regarding products and services, TELCO also provides fixed and mobile telephony, broadband and subscription television. Specifically, the products and services under study are:

- Voice for: fixed line, mobile line and interconnection/roaming
- Data for: fixed line (wholesale/retail), mobile line and interconnection/roaming
- Internet (narrow and broadband)
- Television (with package offers under subscription)
- Package offers
- IT (Information Technology) services (such as outsourcing of systems)
- MVNO (Mobile Virtual Network Operator) services. A MVNO is a mobile operator that provides mobile services to another mobile operator (TELCO). An MVNO pays a determined tariff to such mobile network operator for using the infrastructure to facilitate coverage to its customers. It will be also called carrier services in the study.

Tables 3.3 and 3.4 show the various products and services under the scope of TELCO study.

Table 3.3. TELCO's Products and Services (I)

PRODUCTS AND SERVICES (I)					
Type of p/s (Level 1)		**Category (Level 2)**		**Category (Level 3)**	
1	VOICE	1.1	FIXED LINE	1.1.1	Lines
				1.1.2	Voice services
				1.1.3	Savings plans
				1.1.4	Telephones, Equipment and Maintenance
				1.1.5	Private exchanges
				1.1.6	Booths
				1.1.7	IBERXXX
				1.1.8	Smart network
				1.1.9	Smart network services (voice mail, announcement carrousel, news channels)
				1.1.10	Carrier and Transits
				1.1.11	Services over lines, home security, refill and other services (e.g. multiconference, IP voice, ...)
				1.1.12	Telephone information services
				1.1.13	Telephone cards
		1.2	MOBILE	1.2.1	Contracts
				1.2.2	Prepay
				1.2.3	Associated services (voice mail, video calls, ...)
				1.2.4	Corporate
				1.2.5	Packs
				1.2.6	Terminals
				1.2.7	Other business lines (e.g. network radio)
		1.3	Interconnection / Roaming	1.3.1	Fixed - Fixed
				1.3.2	Mobile - Mobile
				1.3.3	Fixed - Mobile
				1.3.4	Roaming
2	DATA	2.1	MOBILE	2.1.1	SMS (Short Messaging Service)
				2.1.2	MMS (Multimedia Messaging Service)
				2.1.3	"EmoX" (e.g. downloads, games, chat, ...)
				2.1.4	Premium packs
				2.1.5	Blackberry
				2.1.6	Mail Mobile Line
				2.1.7	Data service
				2.1.8	Data cards
		2.2	FIXED LINE (wholesale/retail)	2.2.1	Broadband service
				2.2.2	Connectivity
				2.2.3	Via satellite
				2.2.4	Circuits
				2.2.5	VPN (Virtual Private Network)
				2.2.6	Capacity leasing
		2.2		2.2.7	IP (Internet Protocol) voice
		2.3	Interconnection / Roaming	2.3.1	Fixed - Fixed
				2.3.2	Mobile - Mobile
				2.3.3	Fixed - Mobile
					Roaming

Source: TELCO's information

Table 3.4. TELCO's Products and Services (II)

PRODUCTS AND SERVICES MODEL					
Type of p/s (Level 1)		**Category (Level 2)**		**Category (Level 3)**	
3	INTERNET	3.1	B. NARROW	3.1.1	Access
				3.1.2	Services
				3.1.3	Equipment
		3.2	B. BROAD (wholesale/retail)	3.2.1	ISDN (Integrated Services Digital Services)
				3.2.2	Equipment
				3.2.3	Services
				3.2.4	ISDN + PC
				3.2.5	WiFi zones
				3.2.6	Enterprise solutions
				3.2.7	Net LAN (Local Access Network)
				3.2.8	Loop leasing
				3.2.9	Giga ISDN
				3.2.10	Mega base
4	TELEVISION	4.1	IMAX	4.1.1	ImaX (Basic, family)
				4.1.2	Pay per View/ Video on demand
				4.1.3	Equipment
5	PACKAGE OFFERS	5.1	2P	5.1.1	Voice + Internet
				5.1.2	Voice + Television
		5.2	3P	5.2.1	Voice + Internet + Television
				5.2.2	Voice + Internet + Television + calls to mobiles
		5.3	Response Entrepreneurs	5.3.1	Voice positions
				5.3.2	Computer positions
				5.3.3	Integrated positions
				5.3.4	Options for work positions
				5.3.5	Filter of contents
6	IT SERVICES	6.1	IT SERVICES	6.1.1	Outsourcing of work positions
				6.1.2	Outsourcing of systems
				6.1.3	Systems integration
				6.1.4	Special projects
7	MVNO (Mobile Virtual Network Operator) SERVICES	7.1	For end customer of the reseller	7.1.1	Voice services
				7.1.2	Messaging services
				7.1.3	Data services
				7.1.4	Roaming
				7.1.5	Other services
		7.2	Provided to reseller	7.2.1	Numbering
				7.2.2	SIM card
				7.2.3	Support for end customer
				7.2.4	Migrations
				7.2.5	Portability
				7.2.6	CRM (Customer Relationship Management)
				7.2.7	Voice mail service
				7.2.8	Services for terminals
				7.2.9	Identification of network operator in the terminal
				7.2.10	Technical architecture of the call center
				7.2.11	Relations with third parties
				7.2.12	Support for provision of data connectivity services
				7.2.13	Interception of communications

Source: TELCO's information

In addition to this information about products and services, TELCO has the following main assets for producing them:

- Plant and equipment
    - Power equipment, voice switching equipment and data switching equipment
    - Service platforms and transmission equipment
    - Equipment for radio and satellite
    - Cables, connections and fixed line access equipment
    - Testing systems and customer equipment
    - Mobile access equipment, network circuit switching, network packet switching and network management systems
- Furniture and equipment for information processes
- Other tangible/intangible assets
- Frequencies

The specific scope of the field work applied to TELCO that supports the results and conclusions of this research is defined in the first step of the OpRSA process and also described in the previous sub-section 3.1.1 (methodology). Finally, TELCO's risk management approach under continuous development and improvement is COSO and the reasons for ERM adoption include: legal and market requirements, corporate governance and internal controls re-enforcement, as well as deployment of good practices.

3.2 Operational risk identification and evaluation model

The fundamental and first step in establishing a conceptual model for identifying and evaluating operational risks was to reach a consensus, inside TELCO, on defining the concept of operational risk to be applicable to the telecommunications industry. This definition was done by TELCO's management team considering the concepts defined in COSO (2004, 2017) and ISO 31000 (2009, 2018), and by benchmarking of the financial and banking sector experiences; in this case the definition of operational risk included in Basel II (BCBS, 2006) was revised, prior to this research, by TELCO management team in order to create a common language within the organization to implement an ERM framework which could facilitate the identification and evaluation of TELCO's operational risks. Operational risk was defined as potential losses resulting from events caused by inadequate or failed processes, people, equipment and systems, or from external events. This definition includes compliance risk (the risk of losses arising from violations of, or

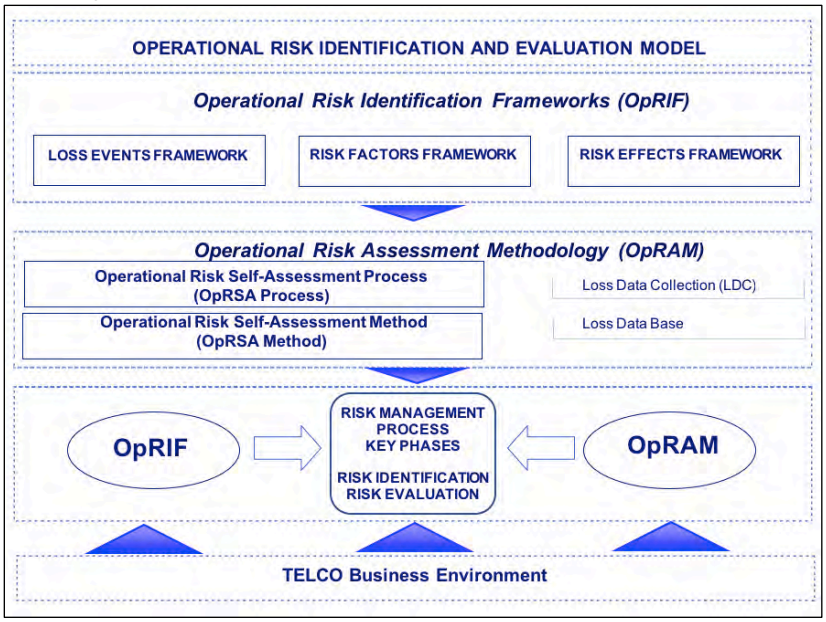
non-conformance with laws, rules, regulations, prescribed practices, internal policies, procedures and ethical standards) but excludes regulatory risks (risk of losses resulting from changes in legislation and regulations related to a given industry or country and that have a relevant impact on the company's activities) as well as strategic risks (risk of losses resulting from wrong decisions about the company's future business plans and strategies). Operational losses include economic, non-economic and reputational effects. Following the definition of operational risk for TELCO, the main objective of this study is the creation of an operational risk identification and evaluation model considering the components of the COSO framework and ISO 31000 standard, in particular, event identification and risk assessment ones. As described in the research methodology, risk identification and evaluation workshops with brainstorming sessions and semi-structured interviews supported by questionnaires were the basic risk assessment tools (ISO 31010, 2009, 2019), in addition to the statistical approach, for building the abovementioned model, as a means of collecting a broad set of data and ideas, ranking them by the managers of TELCO.

The first pillar of the model, operational risk identification (Renn, 2008), allowed a risk typology to classify and identify all operational failures or possible loss events, which is one of the objectives of this study. This was articulated through workshops and semi-structured interviews with the managers of different areas of TELCO, which led to the operational events, risk factors and risk effects frameworks (Gandini *et al.*, 2014; Kozarevic and Besic, 2015). As will be described, it includes the following nine risk type groups: (1) end customer and sale of products and services; (2) poor quality/interruption of service; (3) failures/damage to assets (equipment, networks, systems, facilities, buildings); (4) suppliers, counterparties, contractors and other agents; (5) processes; (6) breach of/non-compliance with laws and standards; (7) fraud and unauthorized activities; (8) employment practices and on-the-job safety; and (9) harm to environment or to third parties. Both the COSO framework and ISO 31000 standard include this identification pillar.

Based on operational risk definition and risk identification frameworks (OpRIF), the second pillar of the model that we created is the operational risk assessment (evaluation) methodology (OpRAM) which embeds two interrelated components: the operational risk self-assessment process (OpRSA process) and the operational risk self-assessment method (OpRSA method). In order to create the OpRAM, and once the risks had been previously identified, detailed facilitated workshops and semi-structured interviews were conducted with TELCO's managers to gather the required information, considering the

best practice of surveying through questionnaires. The survey instrument, based on the control self-assessment technique (Wade and Wynne, 1999; Jacobus, 2015), provided the key inputs for structuring the OpRSA process and method defined in this research. The main data was collected from managers who were considered knowledgeable and reliable informants about risk evaluation process inputs (events impact and likelihood). For every organizational unit under the scope of TELCO case study, a quantitative analysis was performed of subjective estimates the inputs of which are the economic impact and the probability of occurrence of every event for calculating expected, unexpected losses and rating classes for risk evaluation, applying robust actuarial techniques based on scenario analysis. The statistical concepts previously reviewed in the literature were implemented to build the operational risk assessment methodology, where additional references and contents are included further on. Figure 3.3 depicts the operational risk identification and evaluation model developed in this study. The main elements are included in the Model, such as the operational loss event, risk factor and risk effects frameworks (OpRIF pillar) for operational risk identification, as well as the operational risk-self assessment process and method which are the main components of the operational risk assessment methodology (OpRAM pillar). These two pillars led to the composition of the two main phases of the risk management process considered for this study (risk identification and risk evaluation). Furthermore, at the time of this research, no structured loss data was available from TELCO, and this is the reason by which the loss event data capture process (hereinafter LDC) based on the loss database is complementary information useful to be incorporated for enhancing the Model in future research, as explained in the section of conclusions of this study.

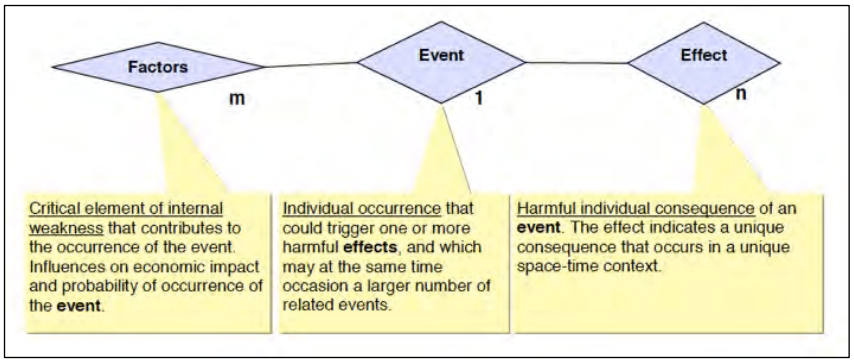
Figure 3.3. Operational Risk Identification and Evaluation Model



3.2.1 Operational risk identification: operational events, risk factors and risk effects identification frameworks for TELCO

The first objective of this research is creating the operational risk identification frameworks (OpRIF) in order to identify operational events, risk factors and risk effects based on TELCO case study. This objective has been developed using the tools, techniques and methods described in the research methodology, mainly through workshops, brainstorming sessions, semi-structured interviews and COSO framework ISO 31000 standard, where the data gathering was supported by the managers of TELCO. The operational risk identification frameworks are the underlying base of the evaluation methodology, the operational risk assessment methodology (OpRAM), and allow and orderly, structured and coherent compilation of data. The operational risk identification frameworks are: (i) the events framework for identifying and classifying all possible types of loss events. It answers the question: "what happened?"; (ii) the risk factors framework for identifying and classifying all causes that gave rise to loss events. It answers the question: "why did it happen?"; and (iii) the effects framework for identifying and quantifying the consequences produces by a loss event. It answers the question: "how much has it cost?" or "how relevant was the impact?". All these frameworks were developed considering TELCO's organization dimension ("where did it occur?"), its assets ("which assets were affected?"), as well as its products and services ("which products and services were affected?") involved in a loss event. These dimensions are summarized in the previous section "TELCO company analyzed". For a proper understanding of the identification frameworks, we created the dimension of the entities (factor, event, effect) of the operational risk and the relation among them, as depicted in Figure 3.4. It shows the interconnection of factors, events and effects. In this way, an event can be associated with "m" factors and "n" effects.

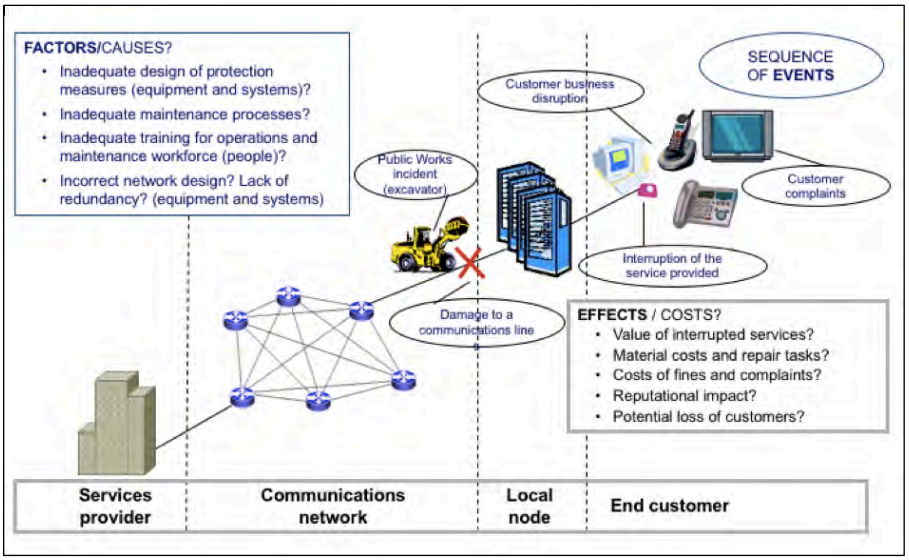
Figure 3.4. Model of Relations among Entities (Factors-Event-Effects)



For a better understanding of these relations, we can consider, as an example, the illustration of the Figure 3.5, where an excavator shovel breaks a communication line by accident. The damage of the line is the incident (event), while there might be various

causes (factors) for this accident such as inadequate design of protection measures of the line or maintenance processes, people failures or even an incorrect network design that should not have been in a place where other maintenance processes performed by other utility companies could take place. In any case, the event led to several consequences (effects) that can even be quantified or qualified such as the value of the interrupted services for other companies, material costs and repair tasks, reputational impacts or even worse, the potential loss of customers due to this failure.

Figure 3.5. Communications Line Factors, Events and Effects. Illustration



These relations among entities (factors, events and effects) are relevant to understand that in order to design any ERM framework or part of it (such as the proposed Model), it is not enough to have a precise definition of the operational risks or even an in-depth knowledge of the multiple loss events that may occur in an organization. It is necessary to have a complete view of the relation among these events, their factors and their effects. This is the rationale of a quality Model.

3.2.1.1 Events framework

The purpose of the events framework is to classify and identify operational failures that serve to analyze the risk in the specific context of TELCO under study through categorization by types of risk. In order to make this research practical and applicable, the criteria for completing the events framework we defined were: (i) it had to be sufficiently extensive and generic to allow all the different events affecting TELCO to be captured, including past events and potential ones; (ii) the descriptions and definitions had to be adapted to the “language”, culture and understanding of the different

businesses and activities of TELCO, so that they were understandable to all managers and end users of the frameworks; and (iii) it had to be designed to optimize and simplify the next pillar of the operational risk identification and evaluation model, i.e. the operational risk assessment methodology (OpRAM). The design would also have to allow future development of the capture of historical data and loss event data capture process. There follows a group-by-group description of the operational events frameworks (classified in three levels of detail) that were validated by TELCO's managers, following the research design methodology.

The first group of the events framework (events at level 1), "end customer and sale of products and services" (Events Group 1), includes those that refer to the relation with the end customer and to the sale of TELCO's products and services. The events are associated with unintentional failures or negligence in the relations with customers, or in the management of the products and services.

Table 3.5. Events Framework (End Customer and Sale of Products and Services)

EVENTS FRAMEWORK					
Event (Level 1)		**Category (Level 2)**			**Category (Level 3)**
1	**End Customer and Sale of Products and Services**	1.1	End customer	1.1.1	Customer data protection claims
				1.1.2	Claims relating to performance/provision of the service (breakdowns, breach of other service levels, quality standards, excluding claims regarding measurement/charging/billing)
				1.1.3	Claims relating to measurement/charging/billing/collection/product or service not recognized
				1.1.4	Claims relating to the customer service (actual and potential)
		1.2	Marketing and sale of products and services	1.2.1	Errors or inaccuracies in the information given to customers
				1.2.2	Errors in capture, recording and maintenance of information used to design products, offers, solutions, prices, services and marketing campaigns
				1.2.3	Errors in identifying, planning and/or launching products, services, solutions, offers and marketing campaigns
				1.2.4	Errors in the design of products, services, offers, solutions marketing campaigns (including loyalty programs)
				1.2.5	Errors/inaccuracies in information recorded on customers/products and/or services contracted
		1.3	Customer service	1.3.1	Error, failure or poor quality in customer care (actual and potential) including post-sale service

The loss events, detailed in Table 3.5 (categories at level 3), are classified into the following risk types (categories at level 2):

- End customer: claims and lawsuits for breach of contractual obligations or lack of quality in the service supplied to customers, including breach of the rules/laws on privacy and protection of the customer.
- Marketing and sale of products and services: errors in the design of offers, products and services (error in capturing information, in the formulas used,...), marketing campaigns, and in the knowledge and advising of customers.
- Customer service: error, failure or poor quality in customer care (current and potential) including post-sale service.

Events Group 2 includes events relating to poor quality or interruption of any of TELCO's products or services to the end customer or to other third parties (e.g. other telecommunications carriers), as well as incapacity to launch the service. The loss events, detailed in Table 3.6 (categories at level 3), are classified into one risk type (categories at level 2): Poor quality/interruption of service: poor quality and delay in the services provided to the end customer or carriers.

Table 3.6. Events Framework (Poor Quality / Interruption of Service)

EVENTS FRAMEWORK					
Event (Level 1)		**Category (Level 2)**			**Category (Level 3)**
2	**Poor Quality/ Interruption of Service**	2.1	Poor quality/ interruption of service	2.1.1	Poor quality associated with the provision of voice, data service, contents (interruption, failures, breach of other service levels, quality standards) due to internal reasons.
				2.1.2	Poor quality associated with the provision of voice, data service, contents (interruption, failures, breach of other service levels, quality standards) due to external reasons (e.g. outgoing interconnection, providers, contractors, customers).
				2.1.3	Poor quality relating to measurement/charging/billing/collection/product or service not recognized.
				2.1.4	Poor quality relating to fraud (spam, phishing).
				2.1.5	Poor quality (including delays) in the provision of new customers / services due to internal reasons (logistical, technical failures).
				2.1.6	Poor quality (including delays) in the provision of new customers/services caused by non-availability of provider.
				2.1.7	Poor quality in execution/repair (except provision new customers/services).

Events Group 3 includes all loss events associated with technical failures and events that involve damage to equipment, to the network, to TELCO's systems and to any company assets. The loss events, detailed in Table 3.7 (categories at level 3), are classified into the following risk types (categories at level 2):

- Accidents: all types of severe/serious accidents.
- Failures: failures or breakdowns in equipment, networks and systems that imply repair or replacement tasks.
- Non-availability: total or partial lack of availability of equipment, networks or systems (due to isolated or simultaneous failures). Total non-availability means that the equipment does not function; partial is when it does not function in optimum conditions.
- Other outside events: rest of external events that involve damage to equipment and systems of TELCO (including acts of vandalism, sabotage and terrorism).

Table 3.7. Events Framework (Failures / Damage to Assets)

EVENTS FRAMEWORK					
Type of event (Level 1)		**Category (Level 2)**		**Category (Level 3)**	
3	**Failures/ Damage to Assets (equipment, networks, systems, facilities, buildings)**	3.1	Failures/damage	3.1.1	System failures.
				3.1.2	Damage in buildings, facilities, merchandise, equipment, networks and vehicles (including electrical and air conditioning/heating equipment).
				3.1.3	Failure in equipment and networks (including electrical and air conditioning/heating equipment).
		3.2	Non-availability	3.2.1	Total non-availability of equipment and systems.
				3.2.2	Partial non-availability of equipment and systems (slow systems, loss of efficiency, communications).
				3.2.3	Non-availability of spare parts for equipment, networks and systems (not including terminals).
		3.3	Other outside events	3.3.1	Intentional damage by third parties to physical assets or software (including actions by employees of other operators).
				3.3.2	Damage caused by animals.
				3.3.3	Unintentional damage caused by third parties.
		3.4	Accidents	3.4.1	Natural disasters.
				3.4.2	Fire in facilities (except natural disasters).
				3.4.3	Flooding in facilities (except natural disasters).
				3.4.4	Collapse of structures and facilities (except natural disasters).
				3.4.5	Other severe equipment failures (except natural disasters).

Events Group 4 includes all events associated with the services received by TELCO from other companies, counterparties and other agents (including competitor companies). These are events relating to non-fulfillment of contractual obligations, as well as possible disputes. The events, as shown in detail in Table 3.8, are classified as follows:

- Non-availability at source: includes events relating to the impossibility of providing contracted services.

- Delays and sub-standard quality in the services received: delays and sub-standard quality in the network services received, construction of new equipment, subcontracted services, replacement of materials and other supplies.
- Conflicts and arbitration in agreements and contracts: contractual and litigious arbitration with business counterparties, suppliers and other agents.

Table 3.8. Events Framework (Suppliers, Counterparties, Contractors and Agents)

EVENTS FRAMEWORK					
Type of event (Level 1)		**Category (Level 2)**		**Category (Level 3)**	
4	**Suppliers, Counterparties, Contractors and other Agents**	4.1	Non-availability at source	4.1.1	Non-availability at source, intermediate or target lines of stocks, spare parts, equipment and systems, supplies and services.
				4.1.2	Interruption of outgoing interconnection service.
				4.1.3	Non-availability of intermediate link lines.
		4.2	Delays and sub-standard quality in the services received	4.2.1	Poor quality of the outgoing interconnection service.
				4.2.2	Errors, failures in the quality of the service due to use of own service by the customer or third parties.
				4.2.3	Errors, failures in the quality of the own service due to use of service of third parties (e.g. carriers).
				4.2.4	Poor quality and delay in construction/installation of new facilities, equipment and systems.
				4.2.5	Poor quality and delay of outsourced services, stocks and materials (non-fulfillment of service levels).
		4.3	Conflicts and arbitration in agreements and contracts	4.3.1	Disputes and arbitration with providers (e.g. breach due to payment delay).
				4.3.2	Disputes and arbitration with contractors.
				4.3.3	Disputes and arbitration with other operators.
				4.3.4	Disputes and arbitration with other agents.

Events Group 5 refers to unintentional failures or errors in the management of processes, operation of equipment and execution, validation, capture and recording of transactions. The events in this group, shown in Table 3.9, can be classified as follows:

- Revenue assurance process: errors in the process of generating revenues, billing and collections for products and services.
- Operation of equipment, networks and systems: events associated with errors in operating company equipment and systems, including errors due to breach of technical limits of company equipment.
- Formalization of contracts: errors and delays in the design, drafting and formalization of contracts, including misunderstandings among companies.
- External and internal disclosure and reporting: errors and delays in reporting to third parties (communication with regulatory organizations, and other agents) and internal reporting within the company.

- Management of investment, stocks, other processes and transactions: errors in other processes and transactions. (e.g. management of investments, management of stocks (routers, terminals), financial contracts and derivatives, and transactions with suppliers of equipment and systems).

Table 3.9. Events Framework (Processes)

EVENTS FRAMEWORK					
Event (Level 1)		**Category (Level 2)**			**Category (Level 3)**
5	**Processes**	5.1	Revenue assurance process	5.1.1	Error in measuring and recording traffic, service, consumption.
				5.1.2	Errors in transfers of CDRs (Customer Data Records).
				5.1.3	Errors in the mediation process.
				5.1.4	Error (incapacity) in discount in prepaid balances of mobile phones.
				5.1.5	Errors in data capture, recording and maintenance (identification of customers, of discounts, of tariffs, rest of service data).
				5.1.6	Errors in charging/assessment contracted service/ application of discounts.
				5.1.7	Billing errors (issuance and sending).
				5.1.8	Collection errors (wrong cutoff, bank orders, duplicate charges).
		5.2	Operation of equipment, networks and systems	5.2.1	Human errors in operating equipment and systems (due to negligence, distraction, overconfidence, lack of qualifications).
				5.2.2	Failures or errors on exceeding technical operating limits of equipment and systems.
		5.3	Formalization of contracts	5.3.1	Errors in design of contracts (including breach counterparties in privacy matters)
				5.3.2	Errors and delays in executing/cancelling contracts.
				5.3.3	Lack of permits, authorizations, powers in contracts (own and third parties).
				5.3.4	Legal documentation; missing or incomplete (including lack of signature or of contract).
				5.3.5	Communication failures.
		5.4	External and internal disclosure and reporting	5.4.1	Lack of reporting or incorrect, incomplete or late reporting (except for mandatory legal reporting).
				5.4.2	Failures or delays in mandatory legal reporting
				5.4.3	Negligent disclosure of confidential information of the company itself.
				5.4.4	Loss or leaks of documents, reports and information.
				5.4.5	Error, lack of alignment or delay in the communication process (e.g. only reactive communication, crisis management, dispersion of channels).
				5.4.6	Errors in implementation, use and application of the brand model.
		5.5	Management of investments, stocks, other processes and transactions	5.5.1	Error in data capture, maintenance, recording and/or recovery (e.g. non-registration of claims, inaccurate information, redundant information).
				5.5.2	Errors and delays in execution.
				5.5.3	Errors and delays in approval.
				5.5.4	Errors in recording the operation.
				5.5.5	Non-compliance with time limits.

Events Group 6 refers to violations of laws and rules, intentional breach of internal policies, as well as improper business practices. As described in Table 3.10, this group includes the following risk types:

- Improper business practices: including infringement of competition law, dubious business practices or abuse of dominant position.
- Intentional breach of internal policies: includes the violation of/non-compliance with internal policies and technical procedures.
- Other violations/non-compliance with laws, regulations and standards: intentional or unintentional violations of rules and laws (telecommunications, accounting, tax regulations, among others) including liability for non-performance of subcontracted services.

Table 3.10. Events Framework (Breach of / Non-Compliance with Laws and Standards)

EVENTS FRAMEWORK					
Event (Level 1)		**Category (Level 2)**			**Category (Level 3)**
6	**Breach of/ Non-Compliance with Laws and Standards**	6.1	Improper business practices	6.1.1	Ignorance/breach of TELCO Principles/Ethics Code or of the policies derived from those Principles. Dubious (unethical) business practices: e.g. billing services that were not contracted, overly aggressive selling, promise of future purchases, offers below cost, breach of deontological codes, misleading advertising, adult-only content, liability in purchases.
				6.1.2	Violation of competition law.
				6.1.3	Abuse of dominant position.
		6.2	Intentional breach of internal policies	6.2.1	Violation/non-compliance internal policies.
				6.2.2	Violation/non-compliance technical procedures.
		6.3	Other violations / non-compliance with laws, regulations and standards	6.3.1	Violation of laws on privacy and protection of data (of customers and employees).
				6.3.2	Violation of laws and regulatory provisions.
				6.3.3	Violation of environmental laws and regulations.
				6.3.4	Violation of accounting and tax laws and regulations.
				6.3.5	Liability with respect to laws and regulations violated by contractors.
				6.3.6	Other legal violations.
				6.3.7	Violation of securities laws (shares and issues of bonds and notes).

Events Group 7 includes intentional acts, with or without willful misconduct, in relation to misappropriation of company property or to violation of the company's internal policies. The risk types included in this group, as described in Table 3.11, are: category includes:

- Internal fraud/unauthorized activities: fraud or unauthorized activities that involve at least one employee of the company (with willful misconduct).

- External fraud: fraud that involves third parties (including contractors), without including damage to assets.

Table 3.11. Events Framework (Fraud and Unauthorized Activities)

EVENTS FRAMEWORK					
Event (Level 1)		**Category (Level 2)**			**Category (Level 3)**
7	**Fraud and Unauthorized Activities**	7.1	Internal fraud/ unauthorized activities	7.1.1	Cloning of cards, terminals and equipment.
				7.1.2	Bad faith manipulation of archives, programs and information (reporting, financial info, customer information).
				7.1.3	Defrauding customers (use of customer rewards, use of other information).
				7.1.4	Theft/extortion.
				7.1.5	Robbing traffic.
				7.1.6	Removal of confidential data, records, program and information (third parties).
				7.1.7	Manipulation of the metering systems.
				7.1.8	Sabotage/malicious destruction of assets.
				7.1.9	Questionable management decisions/conflict of Interests.
				7.1.10	Embezzlement of funds and assets/charging commissions.
				7.1.11	Other types of fraud or unauthorized activities (done by employees).
		7.2	External fraud	7.2.1	Cloning of cards, terminals and equipment.
				7.2.2	Manipulation of electronic and non-electronic information and databases. Removal of confidential data (third parties).
				7.2.3	Defrauding customers (use of customer rewards, use of other information).
				7.2.4	Theft/extortion.
				7.2.5	Robbing traffic.
				7.2.6	Removal of confidential data, records, program and information (third parties).
				7.2.7	Manipulation of the metering systems.
				7.2.8	Distributor fraud (breaking packs, activating cards, selling terminals to the competition).
				7.2.9	Fraudulent contracting/fraudulent use of products (for example, subscription fraud).
				7.2.10	Improper use of TELCO network and of customer resources by customers and third parties (spam, virus attacks, phishing, piracy).
				7.2.11	Harm and violence against employees.
				7.2.12	Other fraud.

Events Group 8 includes events associated with acts that are contrary to the law or to the agreements with employees, as well as those relating to occupational safety and health. The events in this group are classified in Table 3.12 as follows:

- Occupational safety, health and hygiene: events relating to the laws on occupational safety, health and hygiene. Includes all harm or injury suffered by employees. At the time of the field work of this study, the coronavirus COVID-19 crisis did not exist. Otherwise, this risk would have been considered with big impact, not only in the category "Occupational safety, health and hygiene" but also in every operational and no-operational risk classification.
- Relations, diversity and discrimination of employees: relations with the employee, discriminatory conducts and violations of employment laws and contracts, by both parties.

Table 3.12. Events Framework (Employment Practices and On-The-Job Safety)

EVENTS FRAMEWORK					
Type of event (Level 1)		**Category (Level 2)**		**Category (Level 3)**	
8	**Employment Practices and on-the-job Safety**	8.1	Occupational safety, health and hygiene	8.1.1	Employees killed or injured due to accidents (explosion, fire, accidents with vehicles, slips, falls).
				8.1.2	Injuries and disease while performing normal tasks (improper postures, physical overexertion).
				8.1.3	Other events relating to occupational safety, health and hygiene.
				8.1.4	Violence in the workplace.
				8.1.5	Kidnapping and extortion.
		8.2	Relations, diversity and discrimination of employees	8.2.1	Errors in management and/or administration of employee pay, compensation and benefits.
				8.2.2	Strikes and labor conflicts.
				8.2.3	Legal claims/lawsuits with employees.
				8.2.4	Harassment on the job.
				8.2.5	Any type of discrimination (religion, nationality, race, age, gender).
				8.2.6	Interference in private life.
				8.2.7	Impairment of family life due to absence of means for reconciling work and home life.

Events Group 9 includes events associated with harm to the environment or to third parties caused by accidents that may occur in TELCO or through assets of the company. The events are classified following these risk types (described in Table 3.13):

- Environmental damage: including pollution, spills and dumping, and claims due to sensitivity to electromagnetic radiation.
- Damage to third parties and to assets of third parties (excluding employees): damage to third parties and to the assets, facilities, businesses, homes of third parties.

Table 3.13. Events Framework (Harm to the Environment or to Third Parties)

EVENTS FRAMEWORK					
Type of event (Level 1)		**Category (Level 2)**		**Category (Level 3)**	
9	**Harm to the Environment or to Third Parties**	9.1	Environmental damage	9.1.1	Pollution, spills, dumping, recycling, visual impact, noise, consumption.
				9.1.2	Social perception concerning electromagnetic emissions.
				9.1.3	Other environment-related events (e.g. trimming of trees).
		9.2	Damage to third parties and to assets of third parties (excluding employees and customers)	9.2.1	Damage to business continuity, sales and gross margin.
				9.2.2	Harm to persons/animals/live creatures.
				9.2.3	Damage to tangible assets of third parties.
				9.2.4	Damage to intangible assets of third parties (patents, trade secrets, trademarks, copyright, rights of image, design, fraudulent imitation, formats, ideas).

3.2.1.2 Risk factors framework

The purpose of the risk factors framework is to identify the causes (by type) that can trigger the operating loss events described in the operational events framework. The risk factors framework is structured, starting with a classification of the risk factors, in three levels of detail, as well as of four groups of drivers (equipment, systems, products and services; people; processes; and external factors), adapted to TELCO's management structure.

The framework's classification was done considering the following definition criteria:

- It had to be mutually exclusive and collectively exhaustive.
- It should reflect the entire range of risk factors of TELCO, both past and potential. Toward this end, both TELCO's basic and main business, that is, fixed line and mobile telephony, as considered in the scope of the field work under research of this case study.
- The identification and definition of the causes (risk factors) reflected in the framework were designed to allow the adoption of mitigating actions, preparation of action plans, as well as the necessary analysis for optimizing insurance contracts.

There follows a group-by-group description of the risk factors frameworks (classified in three levels of detail) that were validated by TELCO's managers, following the research design methodology.

Factors Group 1 reflects all the causes of operational events related to problems of planning, design, maintenance and security of assets.

The classification of assets was structured following the operational risk-self assessment process (OpRSA) in accordance with the empirical study, i.e. instead of using the categories as defined by TELCO's information in its technical manuals, as described in sub-section 3.1.2.3: (i) plant and equipment (e.g. batteries, protection equipment, international automatic switching equipment, IP network access and transit routers, equipment for television networks management centers, smart network equipment, SMS and MMS centers, submarine network equipment, radio-link systems, submarine cables, testing systems, modems and routers, mobile network management systems,…); (ii) furniture and equipment for information processes (office and storage equipment, management centers, video conference, measurement instruments and devices,…); (iii) other tangible/intangible assets (transport vehicles, right of use and rights in submarine cables…); and (iv) frequencies (mobile network access frequencies, frequencies for multipoint networks, frequencies for transmission networks,…).

In summary, the classification is as described in Table 3.14, where this risk type category includes:

- Planning and development of the investment: factors relating to inappropriate allocation of the investment, and to lack or inadequacy of investment or development plans.
- Design, selection, development/purchase and installation: factors relating to failures or inadequacy in the design and selection, in the development, production and implementation, or in the control of quality, of equipment, systems, facilities, materials and content.
- Maintenance, replacement and obsolescence: factors relating to failures or inadequacy in planning and execution of maintenance and in management of spare parts, as well as those relating to the technical obsolescence of equipment and systems.
- Physical, logical and operational security and business continuity planning: factors relating to lack or inadequacy of controls, security systems, prevention systems, contingency/emergency plans and business continuity planning.

3.14. Risk Factor Frameworks (Equipment, Systems, Products and Services)

RISK FACTORS FRAMEWORK							
Drivers		**Risk Factors (Level 1)**		**Details (Level 2)**		**Details (Level 3)**	
1	**Equipment, Systems, Products and Services**	1.1	Planning and development of the investment	1.1.1	Investment in new equipment, systems, products and services	1.1.1.1	Inadequate allocation/prioritization of investment by investment actions.
						1.1.1.2	Lack of or inadequate planning of investment budgets.
				1.1.2	Development of the Plan	1.1.2.1	Inadequacy or lack of planning of the program/development.
		1.2	Design, selection, development, purchase and installation	1.2.1	Design and selection of equipment, systems, facilities, materials and contents	1.2.1.1	Lack of or inadequate planning in the design and selection of equipment, systems, facilities, materials and contents.
						1.2.1.2	Inadequate design of systems, equipment and facilities (including reliability and redundancy).
						1.2.1.3	Inadequate selection of systems, of equipment (including materials, components) products and services of third parties.
						1.2.1.4	Errors in selection or restrictions in access to contents.
				1.2.2	Development, production and implementation of equipment, systems, facilities, materials and contents	1.2.2.1	Lack of or inadequate planning of development, production or implementation.
						1.2.2.2	Incompatibility of new developments with existing services, products or terminals.
						1.2.2.3	Inadequate execution in development, production or implementation.
				1.2.3	Quality control	1.2.3.1	Lack of or inadequacy of a quality control plan.
						1.2.3.2	Errors in the quality control process (including testing and certification).
		1.3	Maintenance, replacement and obsolescence	1.3.1	Maintenance planning and execution	1.3.1.1	Inadequate planning of maintenance (frequency).
						1.3.1.2	Inadequate definition of maintenance tasks (preventive and corrective), including failures in standardization of tasks.
						1.3.1.3	Failures or inadequacy in execution of maintenance.
						1.3.1.4	Lack or inadequacy of the tools and equipment needed for Maintenance.
						1.3.1.5	Breach of technical limits (e.g. technical hours).
						1.3.1.6	Lack or inadequacy of maintenance policy.
				1.3.2	Stocks of materials	1.3.2.1	Inadequate management of spare parts, replacements and other materials.
						1.3.2.2	Inadequate selection of replacement equipment and materials (including replacement stocks, spare parts and other materials).
				1.3.3	Technical obsolescence	1.3.3.1	Obsolescence of equipment and due to end of technical life (with appropriate maintenance).
		1.4	Physical, logical and operational security and business continuity plan	1.4.1	Security and prevention policies and systems	1.4.1.1	Lack of or inadequate security plans.
						1.4.1.2	Lack of or inadequacy in the prevention and security systems and plans.
						1.4.1.3	Lack of inadequate analysis of impact/selection of critical processes/priorization of risks (vulnerabilities, threats, likelihood).
				1.4.2	Security controls	1.4.2.1	Lack of physical controls (control equipment, security personnel).
						1.4.2.2	Lack (or inefficient monitoring) of logical controls (profiles/users, for access, de detection of intrusions), communication of threats and monitoring).
						1.4.2.3	Lack or inadequacy of operational tests on the controls (physical/logical) for prevention and for security (simulations, revision platform status, upgrades and updating of SW/antivirus).
				1.4.3	Contingency/ emergency/ business continuity planning	1.4.3.1	Lack or inadequacy of plan for incidents/crises/disaster recovery.
						1.4.3.2	Lack or inadequacy of business continuity planning.
						1.4.3.3	Lack or inadequacy of emergency/security equipment.
						1.4.3.4	Lack or inadequacy of backups (including backup sites, alternative lines and other redundancies).

Factors Group 2 includes the risk factors corresponding to operational events relating to problems of qualitative and quantitative sufficiency and employment regulation.

Table 3.15. Risk Factors Framework (People)

RISK FACTORS FRAMEWORK							
Drivers		**Risk Factors (Level 1)**		**Details (Level 2)**		**Details (Level 3)**	
2	**People**	2.1	Qualitative sufficiency	2.1.1	Employee skills	2.1.1.1	Lack or inadequacy of personnel selection/rotation process.
						2.1.1.2	Lack of delegation or adequate leadership.
						2.1.1.3	Lack or inadequacy of training and/or skill building programs (proper and timely training).
						2.1.1.4	Lack or inadequacy of experience in products/services/processes/tasks related to the activities carried on.
						2.1.1.5	Inadequate knowledge of laws and regulations/ internal policies/management of knowledge sharing.
						2.1.1.6	Lack or inadequacy of policy for retaining key Personnel/executive talent.
				2.1.2	Motivation, loyalty of employees	2.1.2.1	Inadequate contract policy and arrangements (salary, incentive system for strategic/commercial skills).
						2.1.2.2	Lack of employee confidence in the management.
						2.1.2.3	Inefficiency or lack of internal communications.
						2.1.2.4	Inadequate work atmosphere (stress level, social climate, interpersonal relations).
						2.1.2.5	Inappropriate work physical environment.
						2.1.2.6	Lack or inadequacy of goals and targets charted (opinion of the workload).
						2.1.2.7	Adverse physiological/psychological state of employees (diminished employee capabilities diminished due to stress, lack of sleep, disease, to his/her acceptance of the job, lack of conciliation).
						2.1.2.8	Lack of employee loyalty to the company.
		2.2	Quantitative sufficiency	2.2.1	Sizing/ Management of organizational units	2.2.1.1	Inadequate number of employees assigned to business units.
						2.2.1.2	Inadequate number of employees in support/ organizational units.
						2.2.1.3	Inadequate control of employee status (leaves, downsizing).
						2.2.1.4	Job absenteeism.
				2.2.2	Allocation of resources	2.2.2.1	Inadequate or incorrect allocation of resources.
						2.2.2.2	Inadequate or incorrect rotation of personnel.
		2.3	Employment law/regulation	2.3.1	Administrative management	2.3.1.1	Inadequate management of employee status in Social Security.
						2.3.1.2	Inadequate management of tax status of employees.
				2.3.2	Legal and contractual matters	2.3.2.1	Inadequate application of contract levels and conditions (salaries and other legal and contractual conditions).
						2.3.2.2	Inadequate management of confidential data of Employee.
						2.3.2.3	Inadequate application of rules on occupational safety, health and hygiene.

As described in Table 3.15, this risk type category includes:

- Qualitative sufficiency: factors relating to employee skills and motivation such as failings or inadequacy in the recruitment process, leadership, delegation, skill building programs, awareness of laws and regulations, internal policies, retention policy for key people, internal communications, goals and targets, and company loyalty, among others.
- Quantitative sufficiency: factors relating to inadequate or incorrect sizing of organizational units and allocation of resources.
- Employment law/regulation: factors relating to inadequate management of administrative, legal and contractual tasks such as inadequate management of social security, tax status, and of confidential data, among others.

Factor Group 3 on processes reflects all causes of operational events relating to problems in the definition of processes and formalization of procedures and controls.

As described in Table 3.16, this risk type category includes:

- Definition of processes: factors relating to lack of or inadequacy in the definition of tasks and activities, in defining and allocation responsibility to the company's organizational structure and adaptation to change.
- Formalization of procedures and controls: factors relating to shortcomings or inadequacies in formalization of procedures, internal communication of manuals, according to the service level between internal units, in controls, and in related action plans.

The category of risk factors associated with processes is the one that has the most interpellations and implications with almost all the events that occur in a company such as TELCO. When we refer to processes we include activities, tasks, responsibilities, organizational aspects, as well as certain procedures. In the fieldwork of the empirical study, the managers who provided information about these events were aware of the difference between what a process and a procedure means, which avoided misunderstanding about the issues to be discussed in this category, both at a general level and at a specific level in other frameworks for identifying operational risks.

Table 3.16. Risk Factors Framework (Processes)

RISK FACTORS FRAMEWORK							
Drivers		**Risk Factors (Level 1)**		**Details (Level 2)**		**Details (Level 3)**	
3	**Processes**	3.1	Definition of processes	3.1.1	Definition of tasks, activities and objectives	3.1.1.1	Failure to identify and define processes, activities and tasks.
						3.1.1.2	Inadequate sequence and hierarchy of processes, activities and tasks.
						3.1.1.3	Lack or inadequacy of definition of indicators and targets.
				3.1.2	Definition and assignment of responsibilities	3.1.2.1	Inadequate identification of responsible persons and players in the process.
						3.1.2.2	Inadequate definition of duties and responsibilities of each function (mission and tasks), including separation of function.
						3.1.2.3	Inadequate definition of hierarchy/authority/permits/powers.
						3.1.2.4	Inadequate or inefficient definition of the reporting chain.
						3.1.2.5	Inadequate internal audit and risk management functions.
						3.1.2.6	Inadequate identification of responsibility for transversal processes.
				3.1.3	Organizational structure	3.1.3.1	Diversity or concentration of geographic/ physical locations.
						3.1.3.2	Complexity of the group structure (subsidiaries, holding companies).
						3.1.3.3	Lack of coordination and diverse criteria between different activities in the structure of the organization.
				3.1.4	Adaptation to change	3.1.4.1	Diversification in innovation of products, service and markets.
						3.1.4.2	Internal reorganization and corporate Activities.
						3.1.4.3	Update, introduction and communication of changes.
		3.2	Formalization of procedures and controls	3.2.1	Formalization of procedures	3.2.1.1	Inadequacy, incomplete status or lack of formalization of procedures (e.g. scaling).
						3.2.1.2	Inadequate internal communication of manuals on procedures.
						3.2.1.3	Redundancy/contradiction of internal policies and procedures.
						3.2.1.4	Inadequate formalization of the service level agreement/interfaces between internal units.
				3.2.2	Quality of the controls	3.2.2.1	Lack of controls.
						3.2.2.2	Ineffectiveness of non-automatic controls.
						3.2.2.3	Ineffectiveness of automatic controls.
						3.2.2.4	Inefficiency, ineffectiveness or lack of reports on control failures.
						3.2.2.5	Inefficiency, ineffectiveness or lack of related action/improvement plan.

Factor Group 4 of external factors reflects all causes of operational events related to the location, the market and regulatory environment and contractors/outsourcing. As described in Table 3.17, this risk type category includes:

- Location: factors relating to exposure to natural disasters and to acts of vandalism, socio-cultural factors, terrorism, and corruption, among others.
- Market and regulatory environment: factors relating to a competitive environment, with business activities and relations with customers and counterparties (discontinuation of activity of a sole/exclusive supplier, provider, and complexity of contractual agreements) and to the socio-political, regulatory and legal environment (inadequate construction of laws, complexity of legislation, and frequency of changes in regulations/laws).
- Contractors and outsourcing: factors relating to contractual agreements, provided services and relations with outside agents (lack of formalization of relations, lack of documentation on penalizations, labor outsourcing, and lack of controls over activities of subcontractors, as well as LOPD-Law of Personal Data Protection-issues).

A common aspect in the identification of events associated with external factors is that the managers interviewed, whenever they proceeded to propose them, associated a cause to justify their proposal. The reason for this is that, unlike other risk categories, these are highly affected by behaviors and situations that are difficult to control, such as exposure to potential external risks associated with exposure to disasters and socio-cultural factors, as well as the competitive environment in the market, the regulatory environment, as well as dependence on third parties in terms of both external agreements and the services provided by them.

One of the factors identified at the time refers to the lack of legal certainty in various business practices. At this point, it is important to highlight the importance of the relationship between the companies and the regulatory bodies, from an ethical and fair point of view. Also noteworthy as an example of these practices is the lack or scarcity of robust regulations that respond to the provision of products and services in the Internet environment. On the other hand, the application of the data protection law should not be used to tighten customer relationship processes, but rather to truly safeguard their physical and intangible assets.

Table 3.17. Risk Factors Framework (External Factors)

RISK FACTORS FRAMEWORK							
Drivers		**Risk Factors (Level 1)**		**Details (Level 2)**		**Details (Level 3)**	
4	**External Factors**	4.1	Location	4.1.1	Exposure to disasters	4.1.1.1	Geographical location liable to suffer natural disasters (earthquakes, volcanoes).
						4.1.1.2	Inadequate protection measures for adverse events (e.g. electrical, environmental).
						4.1.1.3	Adverse environmental and weather situations (rain, lightning)
						4.1.1.4	Excess concentration.
				4.1.2	Exposure to social/cultural factors and acts of vandalism, of terrorism, and to corruption.	4.1.2.1	Adverse social environment, rioting.
						4.1.2.2	Existence of organized terrorism, guerrillas warfare.
						4.1.2.3	Level of tolerance of corruption.
						4.1.2.4	Social and cultural aspects (job absenteeism, language use, manners and customs, environmental awareness).
		4.2	Market and regulatory environment	4.2.1	Competitive environment	4.2.1.1	Degree of market maturity.
						4.2.1.2	Competitive situation in the market.
				4.2.2	Business activities and relations with customers and counterparties	4.2.2.1	Discontinuation of activity of a critical supplier, counterparty, contractor.
						4.2.2.2	Sole/exclusive provider of products.
						4.2.2.3	Suppliers and contractors shared with the competition.
						4.2.2.4	Changes in service providers (maintenance) and product suppliers (spare parts, equipment).
						4.2.2.5	Complexity/fragmentation of products/services in the activity carried on.
						4.2.2.6	Complexity of contractual arrangements with suppliers and Providers.
						4.2.2.7	Insufficiency of investigations prior to non-conventional contracts (on economic impact, legal context).
						4.2.2.8	Propensity of customers and counterparties for legal action.
						4.2.2.9	Incapacity of suppliers to handle company's demand for products, material and equipment.
				4.2.3	Socio-political, regulatory and legal environment	4.2.3.1	Ignorance / inadequate interpretation of laws/regulations.
						4.2.3.2	Complexity of legislation.
						4.2.3.3	Socio-political environment and pressure groups (lack of independence vis-à-vis pressure groups).
						4.2.3.4	Frequency of changes in regulations/laws.
						4.2.3.5	Redundancy/transposition/inconsistency of diverse regulations (local, European).
						4.2.3.6	Legal uncertainty.
						4.2.3.7	Legal defense of consumer interests.
		4.3	Contractors/ outsourcing/ third parties	4.3.1	Contractual arrangement	4.3.1.1	Lack of formalization of relations with the contractor (responsibilities, deliveries).
						4.3.1.2	Single/exclusive service provider
						4.3.1.3	Inadequate capacity to perform contractual obligations.
						4.3.1.4	Personal Data Protection Law (LOPD).
						4.3.1.5	Inadequate definition of the relation with the contractor/ outsourcer/third party or lack of documentation (penalizations, volume rebates, commissions, discounts).
				4.3.2	Services provided	4.3.2.1	Insufficient quality in contracted service.
						4.3.2.2	Lack of controls over activities of subcontractors, as well as operating yardsticks.
						4.3.2.3	Labor outsourcing.
				4.3.3	Relation with contractors	4.3.3.1	Inadequate legal situation of outsourcers and employees.
						4.3.3.2	Lack of or inadequate communication with outsourcers.
						4.3.3.3	Ineffectiveness or lack of records of relevant communications with the contractor.

3.2.1.3 Risk effects framework

The risk effects framework classifies all the operational losses defined for TELCO arising from the operational events analyzed. They are classified in three categories: economic, non-economic and reputational.

Economic Impacts

Economic impact measures monetary losses generated by a specific event. Measuring this impact is important for being able to make efficient estimates of future losses from operational events.

The following economic impacts have been defined in the risk effects framework: (i) direct loss; (ii) loss of profit/loss of revenue; (iii) opportunity costs; and (iv) additional investments. Impacts, effects and examples are shown in Table 3.19. In the scope of this TELCO case study only the first two have been found.

- Direct loss: in this case any confusion between the costs of TELCO's alternatives and the real costs of the operational risk must be eliminated. Direct loss considers effects relating to:
    - losses from damage, theft/robbery or reduction of value of the assets
    - losses associated with items that cannot be considered assets
    - losses associated with employees
    - losses from legal liability, regulatory fines and taxes
    - compensation
    - losses from improper practices or fraud.

In addition, as shown in Table 3.18, Valuation Criteria (VC) have been defined for these direct losses as a critical part of the framework. The study by Swanepoel *et al.* (2017) reviews reputational valuation criteria to measure reputational risk based on a matrix which comprises four key elements: (i) 'who' (e.g. higher-risk customers increasing exposure to a firm's reputational risk); (ii) 'where' (e.g. offshore tax locations may increase evasions risk and therefore reputation impacts would increase); (iii) 'what' (e.g. compliance with law and regulations would enhance a firm's reputation); and (iv) 'how' (any illegal or unethical activities must be discouraged, and adopt best practices to have a recognized company reputation). This is an approach based on a reputational heat map in order to assess the degree of risk posed to reputation.

Table 3.18. Economic Impacts. Cost and Valuation Criteria

Cost	Valuation Criteria
Cost of old equipment/facilities (damage on assets that need to be replaced)	Cost of repair
Cost of new equipment/facilities (new assets and spare parts that must be purchased to replace damaged ones)	Cost of replacement
Cost of spare parts and of repairing materials	Total cost of necessary parts and materials
Labor costs during repair	Cost of labor for performed tasks
Maintenance costs	Cost of special equipment for repair/replacement tasks
Complaints, fines and indemnities	Provisioned total amount for fine and indemnities
Sanctions/judgements (cost of penalties for regulatory infractions)	Provisioned total amount for sanctions/judgements
Employee compensation and legal liability	Damages payable to employees
Cost of third party services (cost of services provided by others such as repair work, advertising expenses, promotion)	Incremental or specific cost of such services
Cost of obsolete stocks	Book value of the stocks (terminals, modems, routers) that are removed

- Loss of profit / Loss of revenue: this consists in the profits TELCO could have obtained in case the operational event did not materialize. The main VC defined for these economic effects can be the following (classified in Table 3.19):
  - Lower revenues. The calculation is as follows:
    - Lower Revenues = Number Customers Affected (#) x [Correct value (€) – Real value (€)]
  - Loss of profit. Two criteria were defined, depending on the type of operational loss event that occurs.

    For the event “End Customer and Sale of Products and Services”, the calculation is:
    - *Loss of Profit = Estimate Customers Lost (#) x Estimated Billing per Customer (€) -Average cost per customer (€)].*

    For the event “Poor Quality and Interruption of Service”, the calculation is:
    - *Loss of Profit = Number Customers Affected (#) x [Average Billing per Customer (€/min.)-Average cost per customer (€)] x Duration of interruption (min.)*

Table 3.19. Effects Framework (Economic Impacts)

EFFECTS FRAMEWORK						
Impact		**Effects (Level 1)**		**Effects (Level 2)**		**Examples**
(Level 0)						
1	**Economic Impacts**	1.1	Direct Loss	1.1.1	Losses due to damages, theft/ robbery or reduction of value of assets (including rights)	Cost of interim solutions to ensure business continuity (e.g. mobile units).
						Cost associated with restoration of facilities and buildings after a disaster or accident.
						Cost associated with loss of asset value.
						Cost of repair work (external or internal).
						Cost of replacing assets or materials stolen/robbed/damaged.
						Cost associated with loss of value due to obsolescence of assets or stocks.
						Cost of attending to and informing third parties after the operational event.
						Cost of loss/destruction of other company property (e.g. databases).
						Cost of obsolete equipment.
				1.1.2	Losses associated with items not classifiable as assets	Cost associated with an error in design or execution of marketing campaigns, market research.
				1.1.3	Economic impacts associated with employees	Cost of harm to employees (pay, compensation, medical attention).
						Cost of temporary replacement staff.
				1.1.4	Legal liability, regulatory fines and taxes	Cost incurred in relation to lawsuits, proceedings or arbitration (including professional fees and trial costs paid, outside legal costs).
						Sanctions and fines.
				1.1.5	Compensation	Cost associated with customer legal complaints/claims (for which the company bears liability).
						Cost due to repayment/replacement of third-party assets.
						Compensation premium due to claims by counterparties (if a final court judgment is entered).
				1.1.6	Losses from improper practices or fraud	Losses from unauthorized activities or businesses.
						Loss due to employee fraud that leads to a loss of profit.
						Loss due to external fraud or to theft/robbery.
		1.2	Loss of profit / Loss of revenue	1.2.1	Lower revenues	Lower revenues due to balances not discounted in prepayment.
						Lower revenues due to errors in the platforms for charging, mediation, transfer of CDR.
						Lower revenues associated with billing errors.
						Lower revenues due to sums not collected or claimed.
				1.2.2	Estimated/Indirect Costs	Loss of profit due to service interruption.
						Loss of profit due to revocation of licenses.
						Loss of profit relating to failure to capture potential customers.
						Loss of profit relating to loss of customers.
		1.3	Opportunity cost	1.3.1	N/A	N/A
		1.4	Additional investments	1.4.1	N/A	N/A

Non-economic impacts

Non-economic impact provides measurements not necessarily related to monetary losses. There may be non-economic impacts that do not directly produce a monetary effect. For example, there may be events with insignificant monetary losses but that have an important effect in other non-economic measures (recovery time, number of customer complaints). This category includes the effects shown in Table 3.20:

Table 3.20. Effects Framework (Non-Economic Impacts)

EFFECTS FRAMEWORK						
Impact (Level 0)		Impact (Level 1)		Effects (Level 2)		Examples
2	**Non-Economic Impacts**	2.1	NA	2.1.1	Loss of capacity	Loss of capacity for an operational event in access/ transport.
				2.1.2	Recovery time	Time needed for repair/replacement of assets/ equipment/systems/networks.
						Breakdown repair time (SLA-Service Level Agreement).
						Service interruption time.
						Time needed for recovery of environment.
				2.1.3	Employees and third parties injured/affected	Number of employees injured.
						Number of other persons injured.
						Number of employees deceased.
						Number of other persons deceased.
						Number of employees affected in their motivation.
						Number of other persons affected (in their assets, business).
				2.1.4	Extent/ area/ length	Area (km2) affected by the service interruption.
						Coverage zones affected.
						Km of network affected.
						Central areas affected.
						Area (km2) affected by contamination.
				2.1.5	Number of customers affected	Number of customers affected.
						Number of claims recorded.
						Number of customers not captured.
						Number of customers lost.
				2.1.6	Loss of service	Voice minutes not provided.
						Number of calls cut off.
						Number of calls not completed.
						Number of calls not serviced.
						Amount of data transmission not provided (MMS, SMS, downloads).
						Number of products not delivered.

Reputational impact

The reputational impact of an operational risk is measured by combining three aspects which were worked on with the managers of TELCO: the generic reputational impact, the qualitative reputational impact and the measuring of reputational impact. This approach was created with the data inputs of the organizational unit of reputation and social responsibility of TELCO, which had previously defined a reputational risk map

based on secondary information from the RepTrak (2016) system which measures a company's ability to deliver on stakeholder expectations, the key dimensions of reputation. Every year, the RepTrak framework and results are prepared by the Reputation Institute which is a data and analytics company that helps global companies to build credibility by providing data-driven insights, using one of the world's largest and highest quality normative reputation databases.

- Generic reputational impact: This is the step where we reviewed the main reputational risks, following the abovementioned dimensions where a set of attributes were identified, as shown in Table 3.21.

Table 3.21. Generic Reputational Impact. Dimensions and Attributes

Dimension	Attribute
Products & Services	Treat customers well
	Good value for money
	Quality of products and services
	Meets needs
	Satisfactory management of claims
	Stands behind quality of its products and services
Workplace	Good employees
	Good place to work
	Rewards employees fairly
	Concern for health and well-being of employees
	Offers equal opportunities
Governance	Responsible use its power in the market
	Ethical behavior
	Open and transparent information
Leadership	Strong and respected leader
	Well organized
	Clear vision of future
Citizenship	Has positive influence on society
	Supports good causes
	Protects the environment
Innovation	Innovative company
	Adapts easily to change
	Launches innovative products and services
Financial performance	Future growth potential
	Generates profits for owners
	Good results

Furthermore, following the research methodology through workshops with managers, we identified, for every type of risk (level 1) and category (level 2), their weighting factors (generic impact) (see Table 3.22).

Table 3.22. Effects Framework. Events and Generic Reputational Impact

Type of event (Level 1)		Category (Level 2)		Generic impact
1	**End Customer and Sale of Products and Services**	1.1	End customer	**49%**
		1.2	Marketing and sale of products and services	**48%**
		1.3	Customer service	**48%**
2	**Poor quality / Interruption of Service**	2.1	Poor quality	**48%**
3	**Failures/Damage to Assets (equipment, networks, systems, facilities, buildings)**	3.1	Failures/damage	**4%**
		3.2	Non-availability	**4%**
		3.3	Other outside events	**4%**
		3.4	Accidents	**4%**
4	**Suppliers, Counterparties, Contractors and other Agents**	4.1	Non-availability at source	**30%**
		4.2	Delays and sub-standard quality in the services received	**30%**
		4.3	Conflicts and arbitration in agreements and contracts	**37%**
5	**Processes**	5.1	Revenue assurance process	**23%**
		5.2	Operation of equipment, networks and systems	**0%**
		5.3	Formalization of contracts	**0%**
		5.4	External and internal disclosure and reporting	**30%**
		5.5	Management of investments, stocks, other processes and transactions	**0%**
6	**Breach of/ Non-Compliance with laws and standards**	6.1	Improper business practices	**45%**
		6.2	Intentional breach of internal policies	**23%**
		6.3	Other violations / non-compliance laws, regulations and standards	**23%**
7	**Fraud and Unauthorized Activities**	7.1	Internal fraud / unauthorized activities	**30%**
		7.2	External fraud	**15%**
8	**Employment Practices and on-the-job Safety**	8.1	Occupational safety, health and hygiene	**27%**
		8.2	Relations, diversity and discrimination of employees	**31%**
9	**Harm to the Environment or to Third Parties**	9.1	Environmental damage	**43%**
		9.2	Damage to third parties and to assets of third parties (excluding employees and customers)	**33%**

- Qualitative reputational impact: The measurement of generic reputational impact obtained on crossing the operational events with the dimensions and attributes of the reputation risk map had to be followed by a qualitative analysis based on the following aspects:
    - Geographic impact: an analysis must be made of whether the effects of the operational event are seen at the local, national, and international level.

- Media coverage: an analysis was conducted of the degree of coverage in newspapers, radio and television, considering readership, audience ratings and level of coverage (local or national).
- Increase in customer claims: an analysis was conducted of the increase in claims due to an individual event with respect to the average obtained from analyzing the last 2-3 years to allow 5 increment ranges to be defined so that the qualitative impact can be classified.
- Loss of customers: an analysis is made of the increase in loss of customers due to an individual event with respect to the average obtained from analyzing the last 2-3 years (considering the evolution of customers) to allow 5 loss-of-customer ranges to be defined so that the qualitative impact could be classified.
- Regulatory investigations: an analysis was made if the event is liable to trigger investigations that can lead to court proceedings. In the OpRSA methodology, the classification was done as a function of the greater or lesser likelihood of occurrence, and in an LDC, the classification would be 4, if regulatory investigations are triggered and 0 otherwise.
- Involvement of senior management: the impact classification was based on the greater or lesser involvement of senior management needed to manage the event.

This analysis serves to express the magnitude of the event, weighted on a reputational impact measurement scale with values ranging from 0 (no impact) to 4 (maximum impact), as shown in Table 3.23. The reputational qualitative impact is obtained as the sum of the impact of each qualitative aspect. The interpretation of this scale is as follows:

- Event qualified as 0: inconsequential impact.
- Event qualified as 1: low impact.
- Event qualified as 2: moderate impact.
- Event qualified as 3: high impact.
- Event qualified as 4: severe impact.

Table 3.23. Qualitative Reputational Impact. Aspects and Events Qualification

Qualitative aspects	**Event i**
1. Geographic impact	[0-4]
2. Media coverage	[0-4]
3. Increase in customer claims	[0-4]
4. Loss of customers	[0-4]
5. Regulatory investigations	[0-4]
6. Involvement of senior management	[0-4]

Source: TELCO's information

- Measuring of reputational impact: After having conducted the analysis of the generic reputational impact calculated with the reputation risk map and the qualitative analysis of the reputational impact, the next step was to calculate the resulting reputational impact, which we will define as the adjusted reputational impact. The adjusted reputational effect is measured from the matrix obtained on crossing the generic reputational impact with the qualitative impact (resulting from the previous evaluation), so that each event is analyzed from a dual perspective: the generic reputational impact (based on its influence on the attributes that affect reputation) and the qualitative impact (on the basis of the magnitude of the event and its effects), i.e.: *Adjusted Reputational Impact = Generic Reputational Impact x Qualitative impact*.

Analyzing the generic reputational of each operational event together with the unit of reputation and social responsibility of TELCO, we found that the greatest impact was defined for events relating to "End Customer and Sale of Products and Services" and to "Poor Quality" for which an impact of close to 50% was obtained.

Six aspects were defined for the qualitative analysis and the measurement scale allowed for values between 0 and 4, so that the highest possible impact for each event was 24. Considering the highest generic reputational impact obtained for operational events, close to 50%, and the highest possible qualitative impact of 24, the current adjusted reputational impact of the events stands at between 0 and 12. As shown in Table 3.24, four ranges were defined for classifying operational events as a function of their reputational effect:

Table 3.24. Adjusted Reputational Impact. Rating

Adjusted Reputational Impact	Rating
[0-3]	Little impact
[3-6]	Medium impact
[6-9]	High impact
[9-12]	Catastrophic impact

Source: TELCO's information

3.2.2 Operational risk assessment methodology: risk self-assessment process and method for TELCO

The second objective of this research is the development and application of an operational risk assessment methodology (OpRAM) which has two components: an operational risk self-assessment process (OpRSA process) and an operational risk self-assessment method (OpRSA method), for evaluating operational risks in TELCO. This objective was developed using questionnaires completed in workshops supported by semi-structured interviews, statistical features on operational loss distributions, risk assessment tools, control self-assessment approaches, as well as actuarial and scenario analysis, and COSO framework and ISO 31000 standard guidelines, among other theories referenced in the following sections, and also described in the research methodology.

The operational risk assessment methodology is based on the identification of the various operational event categories already studied through the operational risk identification frameworks for TELCO, and it is grounded in the following factors: (i) the belief that the opRAM is particularly appropriate to an environment of fast paced business, organizational, and technological changes, since the predictive perspective of the scenario analysis allows such changes to be included immediately in the measurement of risks, whereas in a model based on historical loss data (which in fact where non-existent at the time of this study), there would be some delay (2-3 years); and (ii) the existence of operational risk management methodologies in enterprises of similar characteristics and size of TELCO, for example, in the banking sector, based on Basel Models (BCBS, 2006; 2009; 2011).

The main characteristics of the OpRAM are: (i) involvement of the business units (BUs), in the economic quantification of the risk, following the OpRSA process through estimates of the average economic impact and probability of occurrence of each of the operational events; and (ii) calculation of the economic impact of the risk, applying robust

actuarial techniques (OpRSA method), based on scenario analysis (Fraser and Simkins, 2016), that reflect the risk appetite of each business unit which is analyzed, and provide reliability and credibility and, consequently, the use of the risk measurement for making decisions (Wu *et al.*, 2011).

3.2.2.1 Operational risk self-assessment process

The concept of risk self-assessment process is based on the process of control self-assessment (Arena et al, 2010) which helps in identifying, analyzing, and mitigating risks through cooperative problem solving (Hubbard, 2005). The operational risk self-assessment process (OpRSA process) is articulated in six phases as depicted in Figure 3.6.

Figure 3.6. OpRSA Process

Definition of the scope of the OpRSA process

The activities of this phase are the definition of the approach, top-down (top/middle management involved) vs. bottom up (operational staff); and integral (whole organization) vs. partial (the relevant units of TELCO in terms of potential losses). The identification of the organizational units to be evaluated was decided in this phase. The nature of the different types of operational events made it necessary for their assessment to be done in a single session with the participation of all the people in the business unit with responsibility and knowledge for estimating the inputs of the OpRSA method (average frequency, average severity, and worst case).

For the TELCO field study, a top-down and partial approach has been analyzed, looking for the management commitment and faster implementation of the OpRSA process as well as for being focused on the main segments or organizational units within the business units which generates most of the operational events in the company. In line with the partial approach, the scope of the field study analyzes the main organizational units and segments within the Fixed Line and the Mobile Line business units of TELCO.

Adjustment and parametrization of the OpRSA method

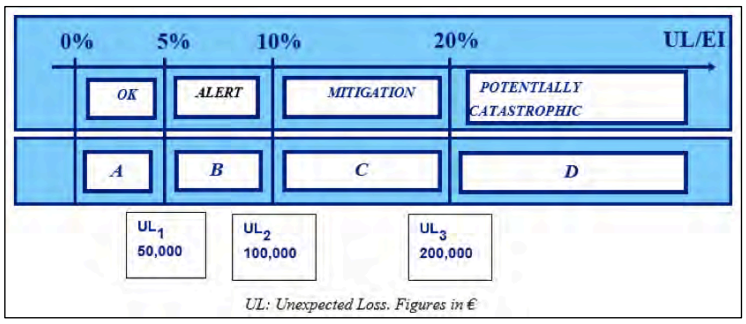
The objectives of this phase are the creation of the questionnaires, the definitions of the risk thresholds (cut-offs) and assessment ranges or risk levels (rating classes), and the setting and parametrization of the calculation engine embedded in the OpRSA method and supported by the OpRSA SW (TELCO's internal software for managing data). The OpRSA method allows an estimate of the economic impact of the risk being evaluated and expressed in terms of expected loss (EL) and unexpected loss (UL). The EL is what TELCO expects to lose in the specified time period. The UL is what TELCO could lose if an unexpected event happens in the business unit.

The core element is the questionnaire, which was designed for each organizational unit or segment, where the event is the driving element. The questionnaires are composed of a number of questions that are put to the managers, who responded for each type of event regarding the estimates. Table 6.1 in Appendix 1 depicts an example of the questions and answers included in the OpRSA SW.

The risk thresholds, which are needed to identify the risk levels (rating classes), are an expression of the risk appetite of TELCO. The objective of the rating process is to associate the risk type to a specific rating class. Since it is difficult to obtain an exact risk measure, it is useful to work with a low number of rating classes. Based on the economic acceptability of certain levels of UL, three risk thresholds (UL1, UL2 and UL3) were defined to establish four rating classes: rating A acceptable (best situation with minimum risk of operational losses), rating B manageable (non-worrisome risk of loss, first sign of alert), rating C critical (problematic situation where a deeper analysis should be performed to evaluate the opportunity of mitigating actions), and rating D catastrophic (very critical situation which needs an immediate mitigating action). The use of ranges to measure risks is described by Hargreaves (2010). When defining risk thresholds, these may be fixed in two ways: (i) with direct identification of an economic sum that is representative of the organizational unit. This amount represents the absolute economic "unexpected losses" related to the business unit's risk appetite; or (ii) with an exposure

indicator, which is the parameter that best represents the business unit's activity in order to define the limit points that mark the different ranges or thresholds. The exposure indicator is basic to provide aggregated information regarding the size of the business unit under analysis, and it should also be a proxy of the effective operational riskiness of the business unit, since only such a driver would allow a meaningful normalization of unexpected loss (UL). More precisely, since the objective of the analysis is the single question (i.e., a single event), UL should be compared to a monetary indicator considered meaningful and able to express the exposure of the business unit for that specific operational loss event. Another relevant aspect in the choice of the exposure indicator is related to its availability in the management information system. For these reasons, accounting indicators are typically used; more specifically P&L (Profit and Loss) measures, since they are particularly good in expressing size and exposure characterizing the operations within a time horizon. Main options for exposure indicators are gross margin, OIBDA, gross revenue, and total costs. The chosen indicator should be representative and reliable of operational volumes expected for the next year. Following this, an exposure indicator (EI) needs to be defined for every business unit. In general, this indicator shows the size of the organizational unit and the risk thresholds are identified by fixing cutoffs (percentages) over these indicators. The normalized measure of unexpected loss (UL) in relation with a risk indicator ratio (UL/EI) allows to create a common scale for all the business units and define "universal" thresholds based on this ratio. Figure 3.7 shows an illustration of risk thresholds, expressed in terms of exposure indicator ratio (UL/EI is expressed in %).

Figure 3.7. Assessment Ranges and Risk Thresholds. Illustration



The risk thresholds based on the OpRSA method used in this study were provided and supported by the finance department of TELCO, and were validated with the managers of the different organizational units and segments (Table 3.27 and Table 3.33 in the sub-section "empirical results" shows the exposure indicators and thresholds of the business units under the scope of the TELCO case study). The risk thresholds of the different business units were established using two exposure indicators, the trade margin for units

with income statements and the operating expenses for the rest of the units. The percentages established in TELCO for the two exposure indicators are presented in Table 3.25.

Table 3.25. Exposure Indicators for TELCO

Threshold	Exposure Indicator	
	Trade Margin	Operating Expenses
Manageable	99%	101%
Critical	98%	103%
Catastrophic	97%	105%

Source: TELCO's data and managers inputs

As an example, if a business unit has a target trade margin of €1000 Million (MM), its thresholds would be established as shown in Table 3.26.

Table 3.26. Thresholds based on Exposure Indicators. Illustration

Exposure Indicator	1000 MM €		
Percentage	99%	98%	97%
Expected value	990 MM €	980 MM €	970 MM €
Threshold	10 MM €	20 MM €	30 MM €

For this business unit, a risk would be considered acceptable if the losses are less than €10 MM, manageable if they are between €10 MM and €20 MM, critical if they are between €20 MM and €30 MM, and potentially catastrophic if they are higher than €30 MM.

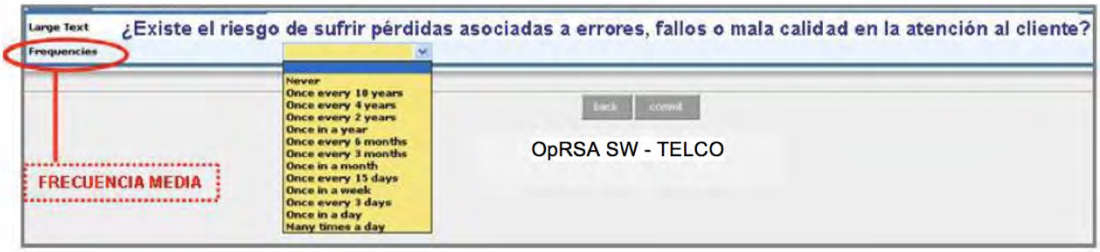
The abovementioned concepts (average frequency, average severity and worst case estimations, risk thresholds, rating classes, expected loss, unexpected loss,…) are explained in detail in the next section, operational risk self-assessment method (OpRSA method), based on statistical features, actuarial approach and the scenario analysis.

Execution of questionnaires

In this phase there is a quantitative answers collection with the business unit managers in terms of mean frequency, mean severity, and worst cases estimates (Barton *et al.*, 2012), which were the inputs of the framework for the scenario analysis performed by the OpRSA method. The process of executing the questionnaires was completed, supported by the OpRSA method and its associated OpRSA SW, as follows:

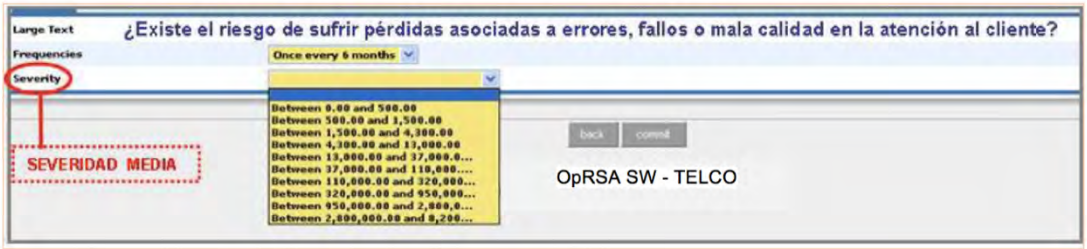
- Once the questions were identified, meetings with the managers were held with the staff of the business unit under study in order to validate the questions and for them to answer.
- For the probability of occurrence (average frequency) of the events, once the risk thresholds were validated by the business units, the question was asked, for every event assigned to the business unit, in terms of the estimated average frequency, i.e., the average number of loss events expected for the considered time period (one year), considering the quality of the existing controls and the available assets.

Figure 3.8. Average Frequency Classes. Illustration. Source: OpRSA SW screenshot



- For the average impact (average severity), after the average frequency question was answered, the managers estimated the average economic severity, defined as the average economic impact expected for an event, considering the existence of controls and recoveries. The severity classes (intervals) are conditioned by the answer provided for the average frequency which helped the manager in the response. For example, the higher the estimated frequency is, the narrower and less economic impact the severity classes are. This is based on the OpRSA method development.

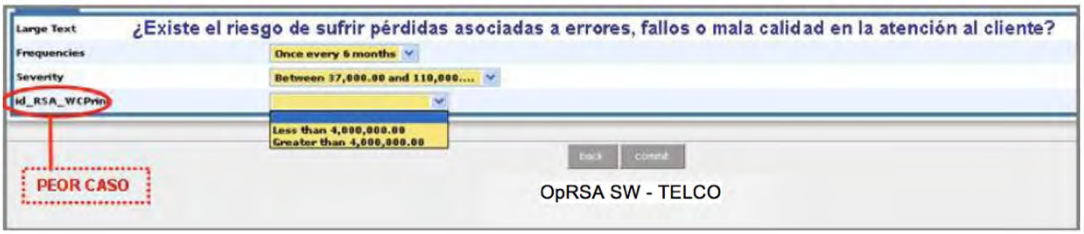
Figure 3.9. Average Severity Classes. Illustration. Source: OpRSA SW screenshot



- Finally, the managers answered the worst case question, which was defined as the economic impact of an event in the worst possible situation. The intervals (classes) offered by the OpRSA method also assisted and facilitated the

managers in making their estimates, which were conditioned by the previous answers on average severity and average frequency.

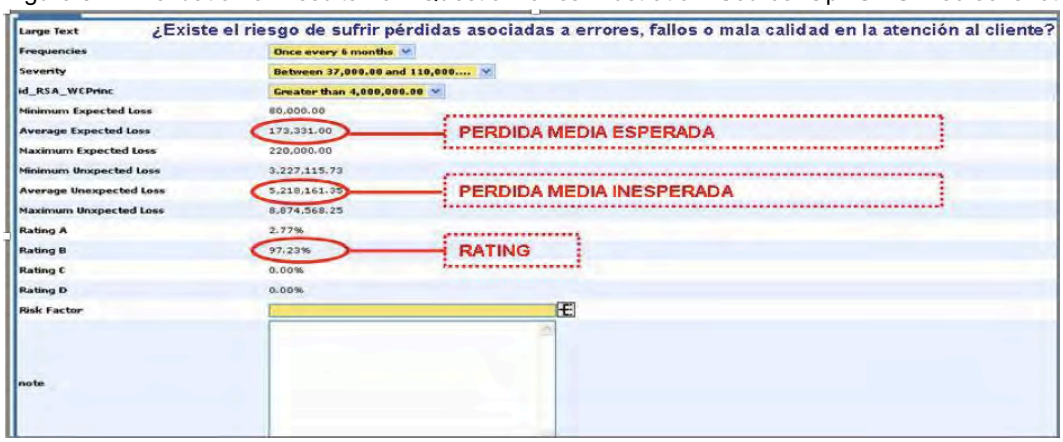
Figure 3.10. Worst Case Classes. Illustration. Source: OpRSA SW screenshot



It is important to highlight that the OpRSA method supported by the OpRSA SW calculation "engine" was the way to gather the data of the three estimates and allowed to turn it into effective information in order to provide the final results for the evaluation of the risks. Furthermore, and as described in the previous illustrations, the OpRSA method facilitated the execution of the questionnaires as every answer for an estimate was based on the previous replies and this made the exercise much easier and quicker for the managers in the data gathering process (see Figure 3.8, Figure 3.9 and Figure 3.10). Fraser (2010) presents relevant information which was useful for conducting the risk interviews.

The last phase of the execution of questionnaires process was the on-site validation of the results obtained when the assessment was completed, providing the average expected losses, the average unexpected losses and the rating (A, B, C and D) obtained, indicating that they were reasonable. Figure 3.11 provides an illustration of this information. This is the essence of the operational risk assessment methodology supported by the OpRSA method.

Figure 3.11. Validation of Results from Questionnaires. Illustration. Source: OpRSA SW screenshot



Review and optimization of the OpRSA process

In this phase, the OpRSA process performed the analysis of results, shared them with the organizational units of the business unit and made the fine tuning of the results and ratings. This phase involved studying the results in order to achieve consistency in terms of expected and unexpected losses and standardized rating. The results obtained in the business unit under study were analyzed by checking them with the audit and finance departments.

Reporting of results of the OpRSA process

This is the phase of the OpRSA process where risk reports are designed, prepared, and shared with the organization. This is relevant for this study to prove the effectiveness of the proposed OpRAM methodology. Reports constitute a reliable tool that provided strategic and operational information, giving a global overview of TELCO's risk exposure to be managed, alerting on anomalous or critical situations, and providing reliable information for making decisions.

Maintenance of the OpRSA process

Basic activities to be included in this phase of maintenance are: periodic review of the OpRAM, review of the level of execution of the questionnaires, update of questions (events in TELCO) included in each questionnaire and risk thresholds, as well as assurance of flow of information to management.

3.2.2.2 Operational risk self-assessment method

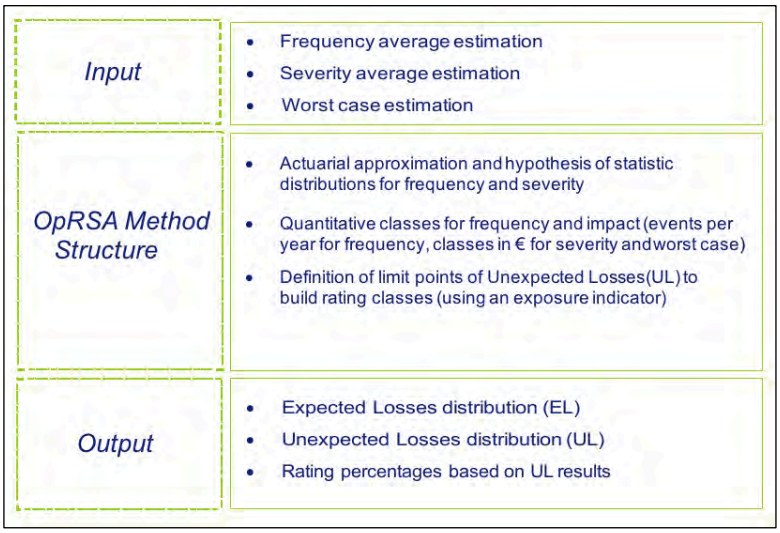
The operational risk self-assessment method (OpRSA Method) consists of a quantitative analysis of subjective estimates (average frequency, average severity, and worst case) collected through the OpRSA process to get an output expressed in terms of risk (unexpected loss). This quantitative analysis is based on an actuarial approach for modelling frequency and severity of risks in order to characterize the potential operational losses. This information, essential to estimate severity dispersion around its mean value, is useful to obtain an output in terms of UL and to define the risk thresholds. The statistical features basics for creating the OpRSA method are described by Basel framework, Chernobai et al (2007), and Strzelczak (2008).

The scheme of the OpRSA method for every event, as shown in Figure 3.12, is defined as follows:

- The inputs are the subjective information coming from the three estimates of the analyzed event (the frequency average, severity and worst case estimations collected from managers through questionnaires as explained in the OpRSA process).
- The outputs are the expected losses (EL) and unexpected losses (UL) distributions density curves, and the rating percentages (risk levels A, B, C or D) based on UL results; i.e. the information needed to evaluate the risks, as it is described in the section of empirical results of this study.
- The scheme structure for transforming the inputs into outputs has been performed through the following elements: as it is further explained, the input estimates are associated with hypotheses on statistical distributions (Poisson for mean frequency; and Weibull for mean severity and worst case) and facilitate, through an actuarial statistical approach known as convolution, the building of a unique loss distribution which shows the expected losses (EL) and unexpected losses (UL) density curves. These density curves provide the outputs of the scheme. However, in order to build them and get to this result, it is necessary to describe the way to define the quantitative classes for frequency and impact (number of events per year frequency, classes in € for severity and worst case), as well as the definition of risk thresholds of normalized unexpected losses (based on appropriate exposure indicators) to build the risk levels (rating classes). This has been developed by transforming a 3-D unexpected loss map, UL surfaces and UL curves in order to finally create the desired EL and UL density curves.

In summary, the theoretical statistical approach developed in the following sub-sections is to turn specific answers of three basic questions into UL and EL density functions to get values from them and the risk thresholds (UL1, UL2 and UL3) to define the risk levels (A, B, C and D). This is useful and relevant information for management about the risk evaluation in order to facilitate the decision making process in a telecommunications company, as discussed in the “interpretation of results for TELCO” section.

Figure 3.12. Scheme of the OpRSA Method



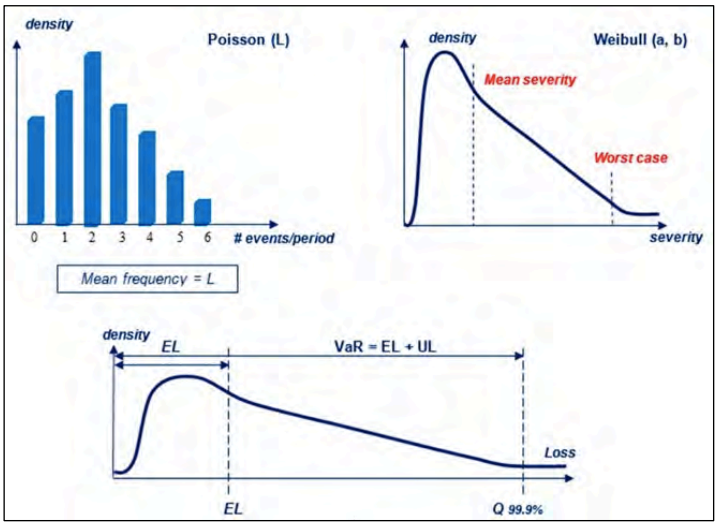
Actuarial approach

The logic of the actuarial approach is to consider separately the distribution of the number of occurrences within a certain time horizon (frequency) and the distribution of the impact of the single event in that period (severity); and then proceed at their convolution to get a unique distribution, the loss distribution, to be cut at the preferred quantile to get the Value at Risk (VaR) at the desired confidence level (Diebold et al, 2000). According to this approach, expected loss-EL is the expected value of the potential loss distribution, while unexpected loss-UL is the difference between the quantile at 99.9% (Value at Risk) of the loss distribution and the expected value of the same loss distribution (EL). It evaluates the degree of dispersion of the distribution in relation to its average value (mean), so it can be considered as a risk measurement (Guillen *et al.*, 2007; and Jobst, 2007). On the other hand, the Capital at Risk (CaR) is identified with the part of the VaR not included in the ordinary activity and therefore not subject to budgeting. Normally, CaR is associated with unexpected loss, with the understanding that the expected loss is covered in the organization's budget.

The following parametric hypotheses have been adopted: for the frequency, that can be described by a single parameter (mean frequency), the Poisson distribution. For the severity, to be described by two parameters, the Weibull distribution (Embrechts *et al.*, 1997), which can be associated with mean severity and worst case, representing quantile at 99.9% on severity distribution. Once the frequency and severity distributions which describe specific loss event types are defined, loss distribution can be obtained via Monte Carlo convolution (Forester *et al.*, 2006). Monte Carlo simulation consists of a random sampling from the severity of many events that have been analyzed according

to the previous chosen sample made on the frequency distribution. Through this distribution, the unexpected loss can be determined at the desired confidence level as shown in Figure 3.13.

Figure 3.13. Convolution of Frequency and Severity Distributions



This means that for each combination (L, a, b) in the 3-D space identified by mean frequency (Poisson-L, mean severity (Weibull-a) and worst case (Weibull-b)), a precise level of expected and unexpected loss can be determined (Martínez-Sánchez *et al.*, 2016).

The next step consisted in identifying in this space all the points with the same level of unexpected loss, defined as “iso-UL surface”. In particular the attention is focused on those three iso-UL surfaces identified by the three critical levels of unexpected loss, coming from the definition of cut-offs on the ratio UL/EI.

Classes for frequency, severity, and worst-case

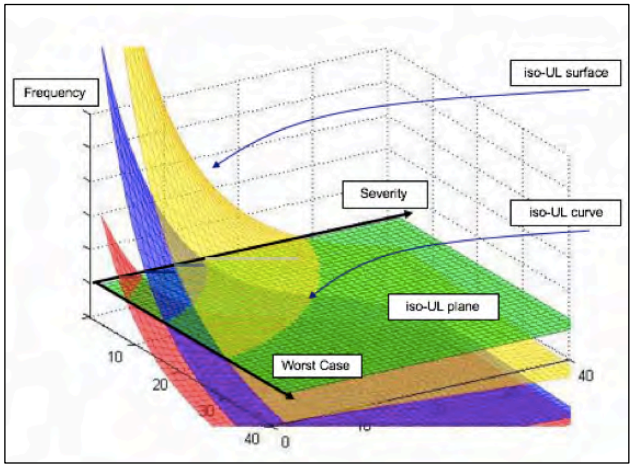
The risk thresholds are based on every business unit depending on their size and their strategic objectives. Therefore, it is necessary to define a measure expressing the risk level that can be associated with a specific risk type and for this reason, the risk thresholds are identified through specific rating classes, where the unexpected loss is the way to represent the risk. Starting from these abovementioned iso-UL surfaces, the rating classes for the collection of the subjective estimates can be determined. The collection of the answers related to frequency corresponds to a mean severity-worst case plane identified by the mean frequency value suggested by the interviewees according to the proposed Table 3.27 as a reference scale.

Table 3.27. Frequency Classes

Frequency Classes (average number events/year)	
Every 10 years	0.1
Every 4 years	0.25
Every 2 years	0.5
Annual	1
Half-yearly	2
Quarterly	4
Monthly	12
Every 2 weeks	26
Weekly	52
2–3 times a week	150
Daily	250
More times a day	500

This plane (iso-UL plane), cutting the iso-UL surfaces, which represent the three critical levels of UL stemming from the cut-offs previously defined, identifies, by intersection, the iso-UL curves which determine groups of points with the same unexpected losses (UL1-the lowest one, UL2-the middle one, and UL3-the highest one, respectively). Figure 3.14 shows the iso-UL surfaces and the iso-UL curves.

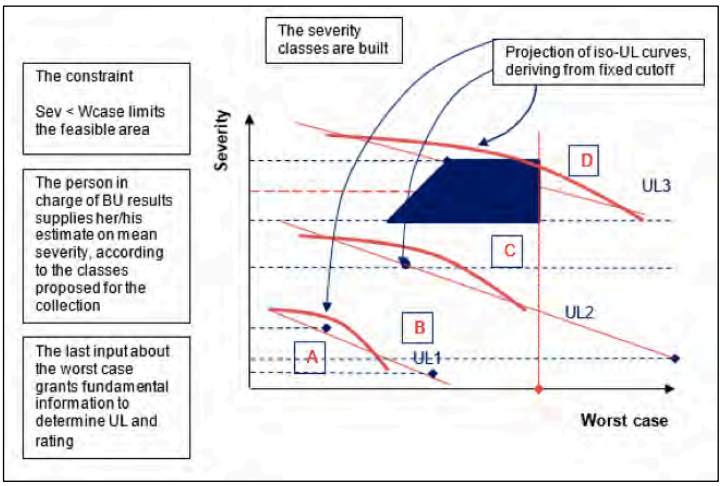
Figure 3.14. iso-UL Map, iso-UL Surfaces and iso-UL Curves



Two properties for these curves emerge: linearity and parallelism. On this plane, the relevant area to be considered for the analysis is limited the following two constraints. First, mean severity $\leq$ worst case (since the quantile at 99.9% on severity distribution is associated to worst case, it is reasonable, by construction, that the mean of this distribution is less than or equal to the worst case itself). Second, mean severity $\leq$ 1/100 worst case (the hypothesis is not to consider too extreme cases in which worst case is equal to more than one hundred times the mean severity). Therefore, the range under analysis is determined considering the upper limit (intersection between bisector – first constraint – and the highest iso-UL curve), and the lower limit (intersection between the lowest constraint and the lowest iso-UL curve), as shown in Figure 3.15. The answer about frequency, together with cut-off on the UL and the abovementioned constraints,

identifies the severity range, on which the severity classes will be concentrated to discern the rating classes.

Figure 3.15. OpRSA Method Constraints for Range Analysis



This aspect is important because it strongly reduces the relevant interval to be considered for severity during the analysis, allowing a limited number of severity classes to be proposed to the interviewee. Moreover, given the size of the organizational unit, the higher the frequency, the smaller the relevant range of severity. This is intuitively correct, since in a situation characterized by high frequency, a small increase in mean severity is enough to have a jump in unexpected loss and a change in the rating class. On the other hand, for high frequencies, the relevant ranges of severity are smaller and also the classes of severity will as a result be narrower. In any case, this is correct and acceptable, since if the interviewee has chosen a very high frequency for loss event under analysis, it is reasonable for this person to have a greater ability of discerning among small severity classes.

Once the relevant range of severity has been determined, the criteria for the determination of the severity classes need to be defined. Severity classes depend on the calibration linked to the size of the unit and on the first answer given to the mean expected frequency for the loss event. In the definition of these division criteria the first choice is related to the number of severity classes to be proposed to the interviewee to collect the subjective estimates. Considering the same relevant range of mean severity, a higher number of severity classes grants the possibility to collect more precise information, while an excessive number of classes makes it objectively more complex to choose when executing the questionnaire, since there is a direct decrease in the wideness of each class, with potential difficulties for the interviewee to answer. The

number of classes adopted has to be sufficient to be able to discern between the different rating classes (the OpRSA SW was parametrized with 8 rating classes); this number is constant, independent from the frequency answer. Once the number of classes to be used has been set, starting from the intersections of the iso-UL curves and the constraints, the identification of the boundaries of each class can be performed in the following way which summarizes the abovementioned criteria: we only keep the three main thresholds deriving from the intersection of the iso-UL curves with the bisector (mean case $\leq$ worst case), and together with the lowest threshold given by the intersection of the first iso-UL curve with the lowest constraint.

The criteria to be followed for the definition of the questions in worst case also need to be defined. The only estimate on the mean severity does not allow to get a full description of the whole distribution of the impact of the single event. This third estimate makes the problem fully determined, allowing a precise identification of a finite area characterizing the set of collected answers (frequency-mean severity-worst case). The intersection between the mean level of the chosen severity class and iso-UL critical curves identifies the thresholds to be proposed for the question in the worst case.

Analysis of the OpRSA method outputs

The subjective estimates treatment of the three parameters and the techniques for output analysis need to be described to understand the results of this study. The answer to each question for frequency, mean severity, and worst case is not punctual, but in classes, so, a priori, loss distribution is not available to determine expected and unexpected loss. The three estimates provided by the interviewee for each risk type allow the individuation of a specific area in the three-dimensional space: the trapezium (area) that represents the aggregated expression of the three collected estimates. Starting from this area, each answer for frequency, severity and worst case can be characterized in terms of expected loss (EL) and unexpected loss (UL).

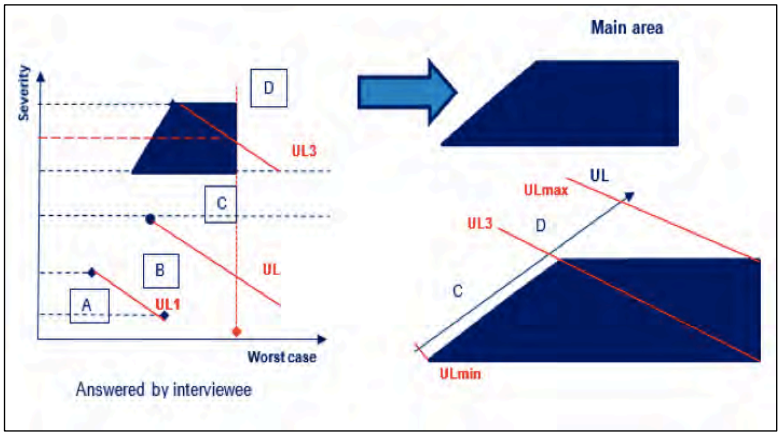
An important hypothesis relating to this area, fundamental to go on with the procedure to get EL and UL, assumes that a uniform distribution has been adopted to describe the probability assigned to each point of the area: each point has the same probability of occurrence as all the others belonging to the area characterized by the same answer. It is clear that, from the general statement of the approach, each point of the analyzed area represents a loss distribution, with a specific expected value (EL) and a quantile at 99.9% (VaR = EL+UL). According to the collected answers, the probability associated to each point is not known. These points are all compatible with the answers, but only one (in

theory) is the “true one”. Modelling the uncertainty of the real point with a uniform distribution, each point of the area has the same probability of occurrence.

The “average severity-worst case” plane to be analyzed after the collection of the first estimate (average frequency) represents a situation of mean frequency by construction and considering the characterized area by the set of answers, the following relation applies: EL = (average frequency) * (average severity); i.e., for each average severity, since the average frequency is constant on this plane, a different level of EL will correspond to it. Based on this, the area under analysis (outputs) can be characterized in terms of expected loss. The information collected through the three subjective estimates can be understood in terms of probability distribution for the expected loss, i.e. a distribution associated to a certain level of probability for each different level of EL coherent with the area under study. This implies that within the severity interval chosen by the interviewee, a distribution can be associated to the analyzed loss event and not simply to a single value of EL.

The characterization of the outputs in terms of UL has the following similar considerations to the abovementioned ideas. As shown in Figure 3.16, moving at constant levels of UL, i.e. parallel to the iso-UL curves, it is easier to identify the areas to be considered. According to this rationale, each answer (frequency – severity – worst case) can be characterized by a distribution of UL. It is important to highlight the fact that even for the UL, the output is not simply a point estimate but a confidence interval.

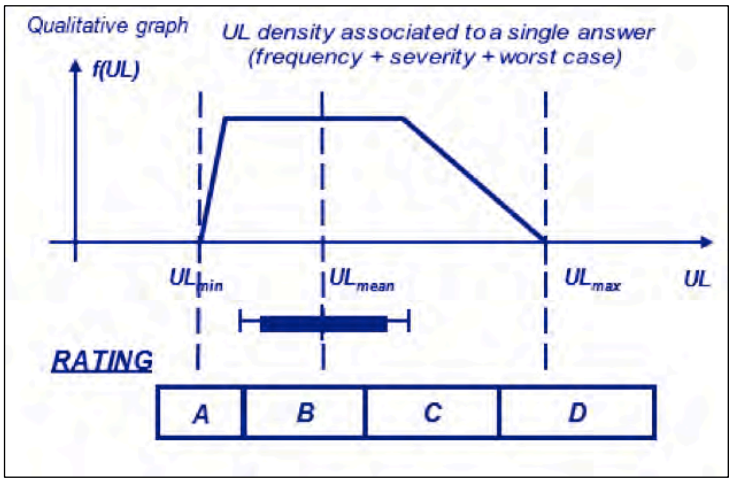
Figure 3.16. OpRSA Method. Output: Unexpected Loss (UL)



As shown in Figure 3.17, the UL distribution obtained from each answer can be aggregated into the total UL distribution related to the whole questionnaire or to a generic group of answers. Aggregation of risk measures is a main pillar for ERM implementation, as described by Brown *et al.* (2019). This distribution represents the basic set of

information used to get aggregated results in terms of total UL (for organizational unit or specific loss event type across the whole organization) and in terms of rating.

Figure 3.17. OpRSA Method. Unexpected Loss Density Function



3.3 Analysis of results

3.3.1 Empirical results

The following results are the empirical outputs applied to the TELCO case study based on the operational risk identification frameworks and implementation of the operational risk assessment methodology, the main components of which are: the inputs from the questionnaires (mean frequency, mean severity, and worst case), the economic evaluation of the results in terms of expected loss (EL) and unexpected loss (UL), the Value at Risk (defined as the sum of EL and UL expressing the maximum expected loss in one year with a confidence level of 99.9%), and the three risk thresholds which identify the four rating classes (acceptable, manageable, critical, catastrophic).

In order to distribute the risk thresholds, defined at business unit level, among the different events included in the questionnaire, a quadratic relationship was used, with the assumption of statistical independence and the same weighting for every event. After calculating the EL and UL for every event, they were compared against the risk thresholds in order to obtain the rating classes. The UL of every individual event is aggregated at the BU type of risk level. For the aggregation at whole BU level, the arithmetic sum is considered. We analyzed the quantitative results described in this section for the following business units under the scope of this study: Fixed line and Mobile line.

The segments or organizational units analyzed in the Fixed Line Business Unit are: Residential; SMEs – Small and Medium Enterprises, Businesses and Professionals (SBP); Carrier Services; Quality, Products and Processes (QPP) and Multimedia. The thresholds for these segments and organizational unit (QPP), and the exposure indicators used in their calculation, are shown in Table 3.28.

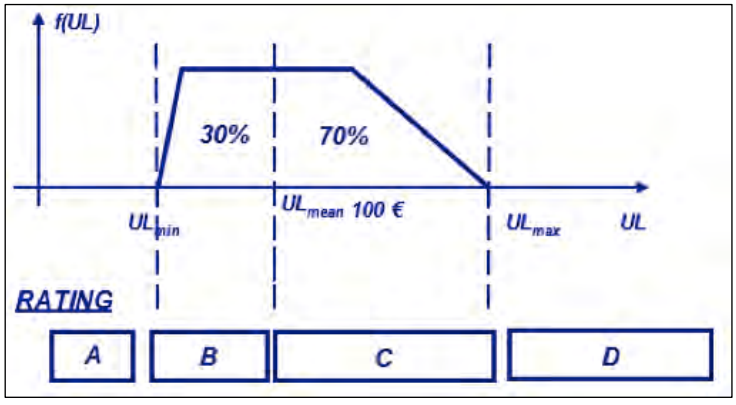
Table 3.28. Exposure Indicators and Thresholds for Fixed Line Business Unit

OpRSA	Exposure Indicator	Threshold 1	Threshold 2	Threshold 3
Fixed Line Business Unit				
Residential	Trade Margin	32,210,000	64,420,000	96,630,000
Professionals (SBP)	Trade Margin	21,800,000	43,590,000	65,390,000
Carrier Services	Trade Margin	10,270,000	20,550,000	30,820,000
Quality, Products and Processes (QPP)	Operating Expenses	3,660,000	10,980,000	18,300,000
Multimedia	Operating Expenses	310,000	590,000	810,000

Source: TELCO's data and managers inputs. Figures in €

When interpreting the information, we need to consider that the results in terms of UL are not represented by punctual data but through a distribution of probability, and therefore when the UL is compared with the risk appetite defined by the BU, this UL distribution surface may be shared among the four different rating classes. Figure 9 shows an example of a type of risk with UL of 100 € and 99.9% of confidence level, where the results are: 30% probability rating B (manageable) and 70% probability rating C (critical). Rating D means potentially catastrophic.

Figure 3.18. UL Density Function and Rating Classes. Illustration



In the case of the application of the OpRSA methodology to the Residential segment of the fixed line, the results are shown in Table 3.29.

Table 3.29. Results of Residential Segment of Fixed Line

EVENT TYPE		TYPE 1	TYPE 2	TYPE 4	TYPE 5	TYPE 6	TYPE 7	TOTAL
		End Customer	Poor Quality	Suppliers	Processes	Non-compliance	Fraud	
TOTAL	EL	28,060,000	84,490,000	2,540,000	3,730,000	40,000	2,820,000	121,670,000
	UL	8,000,000	19,780,000	5,540,000	17,920,000	1,380,000	2,840,000	55,460,000
	Rating A	**100.00%**	0.50%	**81.20%**	41.00%	**100.00%**	**100.00%**	
	Rating B		**94.40%**	18,80%	**59.00%**			**94.00%**
	Rating C		0.90%					6.00%
	Rating D							
	UL.I	16,820,000	13,730,000	6,870,000	16,820,000	9,710,000	9,710,000	32,210,000
	UL.II	33,640,000	27,470,000	13,730,000	33,640,000	19,420,000	19,420,000	64,420,000
	UL.III	50,460,000	41,200,000	20,600,000	50,460,000	29,140,000	29,140,000	96,630,000

Source: outputs of OpRSA SW and author's own elaboration. Figures in €

The Residential segment of the fixed line estimated an average expected loss of 122 MM € in one year, and an average unexpected loss of 55 MM €; the rating classes defined the situation as manageable (94%) based on the risk thresholds proposed by the unit (32 MM €, 64 MM €, and 96 MM €), which indicated a non-worrisome loss, just a first sign of alert. A global result was found where the unexpected loss was lower than the expected loss. This indicated an overall events typology characterized by a high frequency with a limited severity (small/medium). In this case, the mitigating actions had to be focused on main events to solve failures in order to reduce the probability of occurrence of the events and the associated losses. Analyzing the types of events, it was found that the "poor quality" event (risk type 2), together with the "processes" event (risk type 5) had a manageable classification, the rest of them being acceptable (risks types 1, 4, 6, and 7). The Residential segment was mainly oriented to commercial activities and this is the reason why "poor quality" had more importance than the rest of them. The expected and unexpected losses of this event showed, respectively, 69% and 35% over the total unit. Based on the identification of events, "poor quality" had four associated risks: "poor quality in the service provision due to internal causes" of TELCO, "poor quality in the service provision due to external causes", "poor quality in the service provision for new customers" and "poor quality due to the rest of causes (interruptions, fraud and billing, as most relevant). The "poor quality in the service provision due to internal causes", with an expected loss of 42 MM €, represented the largest expected loss in the Residential segment. It had an unexpected loss of 5 MM €, far below the expected loss, which implied that the event had a high frequency of occurrence, as well as a medium or low impact every time it was materialized. The main "poor quality event due to internal causes" was the churn of customers and the ARPU (Average Revenue Per User) was the impact variable. The largest unexpected loss event was "poor quality

in the service provision for new customers", 17 MM € as unexpected loss, being a critical rating class. As the expected loss was 14 MM €, it could be considered that this event had lower frequency and bigger impact than the previous one. Finally, within the "processes" type, the event "errors and delays in the formalization of contracts" was evaluated, with a critical rating class (56%) and 17 MM € of unexpected loss, eight times higher than the expected loss. This is a low frequency event, once every two years, a with big impact. The interviewed managers argued about the lack of updated contracts with their suppliers due to different reasons.

In the case of the application of the OpRSA methodology to the SMEs – Small and Medium Enterprises, Businesses and Professionals (SBP) segment of the fixed line, the results are shown in Table 3.30.

Table 3.30. Results of Professionals (SBP) Segment of Fixed Line

EVENT TYPE		TYPE 1	TYPE 2	TYPE 4	TYPE 5	TYPE 6	TYPE 7	TOTAL
		End Customer	Poor Quality	Suppliers	Processes	Non-compliance	Fraud	
TOTAL	EL	4,180,000	400,000	240,000	2,460,000	740,000	2,003,000	10,050,000
	UL	10,840,000	2,830,000	2,420,000	7,560,000	11,340,000	7,430,000	42,410,000
	Rating A	**63.00%**	**98.00%**	**100.00%**	**98.00%**		29.00%	
	Rating B	37.00%	2.00%	8.00%	2.00%	10.00%	**71.00%**	**62.00%**
	Rating C					**88.00%**		38.00%
	Rating D					3.00%		0.00%
	UL.I	11,380,000	9,300,000	4,650,000	10,390,000	6,570,000	6,570,000	21,800,000
	UL.II	22,760,000	18,590,000	9,290,000	20,780,000	13,140,000	13,140,000	43,590,000
	UL.III	34,150,000	27,880,000	13,940,000	31,170,000	19,720,000	19,720,000	65,390,000

Source: outputs of OpRSA SW and author's own elaboration. Figures in €

The Small and Medium Enterprises, Businesses and Professionals (SBP) of the fixed line segment estimated an average expected loss of 10 MM € in one year, and an average unexpected loss of 42 MM €; the rating classes defined the situation as manageable (62%) based on the risk thresholds proposed by the unit (21 MM €, 43 MM €, and 65 MM €), which indicated a non-worrisome loss, just a first sign of alert (furthermore, the situation is considered as critical at 38% of probability). It was found a global result where the unexpected loss was higher than the expected loss. This indicated an overall events typology characterized by a medium/low frequency with a medium/high impact. severity (small/medium). This makes sense as the number of customers in this segment is much lower than in the Residential segment and with higher size in terms of sales income. Analyzing the types of events, it was found that the "breach of/non-compliance with laws and standards" event (risk type 6) had a critical classification, "fraud and unauthorized activities" event (risk type 7) a manageable

classification and all the rest of events were acceptable. The event “breach of/non-compliance with laws and standards” had an expected loss of 0,7 MM € and an unexpected loss of 11 MM €, meaning a low frequency and high impact risk; the mitigating actions for such a risk should be focused on reducing the severity more than the probability of occurrence, and they are difficult to be implemented as well as costlier than the risk materialization itself. The risk associated with this type is “intentional breach of internal policies” with a critical classification. This leads to the need of performing an in-depth analysis to consider a mitigating action, as it is an internal issue of the company, and therefore, manageable. The managers argued as causes of this event, the employees lack of ability and the insufficient controls quality. Finally, the event “fraud and unauthorized activities” had an expected loss of 2 MM € and an unexpected loss of 7,4 MM €. The main risk is the “external fraud” with 6,7 MM of unexpected loss and 1,8 MM € of expected loss, being classified as manageable. Again, as discussed with the managers, the mitigating actions for managing this risk are more expensive that the risk itself.

In the case of the application of the OpRSA methodology to the Carrier Services segment of the fixed line, the results are shown in Table 3.31.

Table 3.31. Results of Carrier Services Segment of Fixed Line

EVENT TYPE		TYPE 1	TYPE 2	TYPE 5	TOTAL
		End Customer	Poor Quality	Processes	
TOTAL	EL	110,000	410,000	430,000	960,000
	UL	1,600,000	1,550,000	3,200,000	6,350,000
	Rating A	**100.00%**	**97.30%**	**100.00%**	**100.00%**
	Rating B		2.7.00%		
	Rating C				
	Rating D				
	UL.I	5,930,000	2,420,000	5,930,000	10,270,000
	UL.II	11,860,000	4,840,000	11,860,000	20,550,000
	UL.III	17,790,000	7,260,000	17,790,000	30,820,000

Source: outputs of OpRSA SW and author’s own elaboration. Figures in €

The Carrier service segment estimated an average expected loss of 1 MM € in one year, and an average unexpected loss of 6 MM €; the rating classes defined the situation as acceptable which means an optimum situation with minimal risk of operating losses. The results showed an unexpected loss more than six times higher than the expected loss, so that the overall risk has a low frequency and high impact. This is reasonable considering the limited number in terms of customers and size, so that the risk impact related to them is very high. After analyzing the risk types, all of them can be classified

as acceptable. It should be noted that for the “processes” event, the unexpected loss is 50% of the total unexpected loss of the segment, while the expected losses represent 44% of total.

In the case of the application of the OpRSA methodology to the Quality, Products and Processes (QPP) organizational unit of the fixed line, the results are shown in Table 3.32.

Table 3.32. Results of Quality, Products and Processes (QPP) Organizational Unit

EVENT TYPE		TYPE 1	TYPE 5	TYPE 6	TYPE 7	TOTAL
		End Customer	Processes	Non-compliance	Fraud	
TOTAL	EL	10,000	50,000	100,000	1,000	160,000
	UL	690,000	1,170,000	890,000	80,000	2,840,000
	Rating A	**99.80%**	**100.00%**	**97.30%**	**100.00%**	**89.30%**
	Rating B	0.20%	0.00%	2.70%		10.70%
	Rating C					
	Rating D					
	UL.I	1,490,000	2,110,000	1,490,000	2,110,000	3,660,000
	UL.II	4,480,000	6,340,000	4,480,000	6,340,000	10,980,000
	UL.III	7,470,000	10,570,000	7,470,000	10,570,000	18,300,000

Source: outputs of OpRSA SW and author’s own elaboration. Figures in €

The Quality, Products and Processes (QPP) organizational unit estimated an average expected loss of 0,16 MM € in one year, and an average unexpected loss of 2,8 MM €; the rating classes defined the situation as acceptable which means an optimum situation with minimal risk of operating losses.

The rationale behind this risk assessment is due to the treatment which was given to the support units. The risks of this organizational unit are the results of claims, errors in the design of products and services, as well as errors in the revenue assurance process, measuring and recording traffic. These risks are managed by this unit, but they are included in the questionnaires for every business unit.

In the case of the application of the OpRSA methodology to the Multimedia segment of the fixed line, the results are shown in Table 3.33.

Table 3.33. Results of Multimedia Segment of Fixed Line

EVENT TYPE		TYPE 1	TYPE 2	TYPE 5	TYPE 6	TYPE 7	TOTAL
		End Customer	Poor Quality	Processes	Non-compliance	Fraud	
TOTAL	EL	90,000	10,000	100,000	4,000	10,000	210,000
	UL	170,000	50,000	210,000	50,000	50,000	540,000
	Rating A	40.20%	**100.00%**	4.30%	**98.40%**	**100.00%**	
	Rating B	**59.80%**		**95.70%**	1.60%	**71.00%**	**88.30%**
	Rating C						11.70%
	Rating D						
	UL.I	170,000	110,000	180,000	110,000	110,000	310,000
	UL.II	320,000	200,000	350,000	200,000	200,000	590,000
	UL.III	440,000	280,000	480,000	280,000	280,000	810,000

Source: outputs of OpRSA SW and author's own elaboration. Figures in €

The Multimedia segment (internet portals) estimated an average expected loss of 0,2 MM € in one year, and an average unexpected loss of 0,54 MM €; the rating classes defined the situation as manageable, which indicated a non-worrisome loss, just a first sign of alert. In accordance with the managers' inputs, this result is based on the emerging multimedia projects. Even though the dominant classification is manageable, the complete interpretation is the following; there is an 88% probability that unexpected losses can be considered acceptable, while there is a probability of 12% for them to be analyzed as critical. Two events typologies have been identified as manageable, "end customer" and "processes", while the rest of the events are classified as acceptable.

In the "processes" event, there were two risks which imply major losses. The risk "errors in measuring and recording traffic, service, consumption" has an expected loss of 0.053 MM €, an expected loss of 0,11 MM €, which was classified as acceptable (rating B 95.70%). It is a low frequency risk, four times a year, but as argued by the managers in the questionnaires execution meeting, this process is performed by an external company and the decision was to accept this risk. There was no possibility to be measured by another company, and in the case of discrepancies, TELCO has to accept the external assessment. The other "processes" risk was "formalization of contracts" with an expected loss of 0,044 MM € and an unexpected loss of 0,17 MM €, classified as critical. The managers considered the compensation costs for assuming responsibilities and obligations for errors and delays of executing or cancelling the contracts, as well as the loss of profit due to those delays. The cause for this was argued in terms of inadequate processes of TELCO for the situation of the Multimedia segment regarding the contracts formalization. The mitigating action was directed towards the process redesign about contracts formalization and authorization.

In the "end customer" event, the risk with major loss was "marketing and sales of products and services" with an expected loss of 0,087 MM € and an unexpected loss of 0,17 MM €, classified as critical (rating B 59.80%). It has a low frequency, four times a year, and it is mainly due to delays in the launching of the marketing campaign as a result of errors in the service suppliers selection. Mitigating actions were aimed at setting quality controls in the process for selecting the right suppliers.

The segments or organizational areas analyzed in the Mobile Business Unit are: Residential; Sales; SMEs – Small and Medium Enterprises, Businesses and Professionals (SBP) and Wholesale Business. The thresholds for these segments and the exposure indicators used in their calculation are shown in Table 3.34.

Table 3.34. Exposure Indicators and Thresholds for Mobile Line Business Unit

OpRSA	Exposure Indicator	Threshold 1	Threshold 2	Threshold 3
Mobile Line Business Unit				
Residential	Trade Margin	29,150,000	58,290,000	87,440,000
Sales	Operating Expenses	15,900,000	47,700,000	79,500,000
Professionals (SBP)	Trade Margin	14,520,000	29,050,000	43,570,000
Wholesale Business	Trade Margin	2,080,000	4,160,000	6,250,000

Source: TELCO's data and managers inputs. Figures in €

In the case of the application of the OpRSA methodology to the Residential segment of the mobile line, the results are shown in Table 3.35.

Table 3.35. Results of Residential Segment of Mobile Line

EVENT TYPE		TYPE 1	TYPE 2	TYPE 4	TYPE 5	TYPE 7	TYPE 9	TOTAL
		End Customer	Poor Quality	Suppliers	Processes	Fraud	Harms	
TOTAL	**EL**	5,900,000	39,980,000	13,350,000	930,000	4,210,000	480,000	64,860,000
	UL	11,810,000	27,270,000	9,840,000	4,900,000	2,800,000	3,600,000	60,220,000
	Rating A	**99.50%**		**58.70%**	**100.00%**	**100.00%**	**97.90%**	
	Rating B	0.5%	12.50%	41.30%			2.1%	33.60%
	Rating C		**87.40%**					**66.40%**
	Rating D		0.20%					
	UL.I	15,740,000	11,900,000	10,310,000	14,580,000	8,410,000	5,950,000	29,150,000
	UL.II	31,480,000	23,800,000	20,610,000	29,150,000	16,830,000	11,900,000	58,290,000
	UL.III	47,220,000	35,700,000	30,910,000	43,720,000	25, 240,000	17,850,000	87,440,000

Source: outputs of OpRSA SW and author's own elaboration. Figures in €

The Residential segment of the mobile line estimated an average expected loss of 64,8 MM € in one year, and an average unexpected loss of 60 MM €; the rating classes defined the situation as critical based on the risk thresholds proposed by the segment (29 MM €, 58 MM €, and 87 MM €) which led to performing an in-depth analysis to consider mitigating actions. The results show that the unexpected loss is lower than the expected loss, which means that this risk typology is characterized by a high probability of occurrence and a medium-low severity. This happens when a process is executed many times with failures. In this case, the mitigating actions should be focused on identifying the failed process and solving the issue in order to reduce its frequency and therefore, the associated loss. Analyzing the various types of events, we found the "poor quality" event is the only one classified as critical, the rest of them being acceptable. The residential segment of the mobile line is mainly focused on the commercial aspect, and this is the reason for which the "poor quality" event has more impact than the rest of the risks. The expected and unexpected losses of this event represent 61% and 45% respectively over the total of the segment. The "poor quality" has four associated risks: "poor quality in the service provision due to internal reasons", "poor quality in the service provision due to external reasons", "poor quality in the service provision to new customers", and "poor quality due to the rest of the causes (repair, fraud, charging and billing,…). The "poor quality" due to internal reasons, with an expected loss of 23 MM €, represents the major expected loss in this segment. It has an unexpected loss of 22,9 MM €, similar to the expected loss, which means that the event has a high probability of occurrence and a medium-low impact every time the risk materializes. For this reason, this event is classified as potentially catastrophic (rating D).

In the case of the application of the OpRSA methodology to the Sales organizational unit of the mobile line, the results are shown in Table 3.36.

Table 3.36. Results of Sales Organizational Unit of Mobile Line

EVENT TYPE		TYPE 1	TYPE 2	TYPE 4	TYPE 5	TYPE 7	TOTAL
		End Customer	Poor Quality	Suppliers	Processes	Fraud	
TOTAL	EL	480,000	4,200,000	80,000	5,170,000	2,00,000	11,930,000
	UL	2,380,000	14,260,000	80,000	8,310,000	930,000	25,960,000
	Rating A	**94.00%**		**100.00%**	40.00%	**100.00%**	0.3%
	Rating B	6.00%	16.00%		**60.00%**		**97.70%**
	Rating C		**62.70%**				6.00%
	Rating D		21.30%				
	UL.I	4,910,000	3,470,000	6,010,000	7,760,000	9,180,000	15,900,000
	UL.II	14,720,000	10,410,000	18,030,000	23,280,000	27,540,000	47,700,000
	UL.III	24,530,000	17,350,000	30,050,000	38,790,000	45,900,000	79,500,000

Source: outputs of OpRSA SW and author's own elaboration. Figures in €

The Sales organizational unit of the mobile line estimated an average expected loss of 11,9 MM € in one year, and an average unexpected loss of 25,9 MM €; the rating classes defined the situation as manageable. All events have been classified as acceptable, except for “poor quality” (critical) and “processes” (manageable).

The event “poor quality”, associated with logistics and technical failures, and unavailability of providers, were classified as critical (62%), with an expected loss of 4,2 MM € and an unexpected loss of 14,2 MM €, which means 35% and 55% of the total, respectively. The managers argued that the most relevant event associated with this risk is the stock out from providers, mainly in seasons with high demand such as Christmas or summer; for this reason, the frequency is considered twice a year. Some ideas for mitigating actions in order to solve the stock out is offering more expensive subsidized smartphones to avoid these inconveniences for potential customers.

The event “processes” was classified as manageable, with 5,3 MM € of expected loss and 8,3 MM € of unexpected loss, due to the complexity of the commission settlement processes with the distribution channel (data collection and maintenance, approval of operations, information register, failure to meet deadlines,…). The classification of this risk is manageable. The rest of the risks associated with the investment management, stocks, other processes and transactions obtained the classification of acceptable.

In the case of the application of the OpRSA methodology to the SMEs – Small and Medium Enterprises, Businesses and Professionals (SBP) segment of the mobile line, the results are shown in Table 3.37.

Table 3.37. Results of Professionals (SBP) Segment of Mobile Line

EVENT TYPE		TYPE 1	TYPE 2	TYPE 4	TYPE 5	TYPE 7	TOTAL
		End Customer	Poor Quality	Suppliers	Processes	Fraud	
TOTAL	EL	6,060,000	10,000	1,590,000	450,000	170,000	8,280,000
	UL	2,780,000	30,000	10,890,000	2,420,000	110,000	16,240,000
	Rating A	**100.00%**	**100.00%**		**100.00%**	**100.00%**	20.10%
	Rating B			37.00%			**79.90%**
	Rating C			**63.00%**			6.00%
	Rating D						
	UL.I	7,840,000	5,930,000	5,130,000	7,260,000	4,190,000	14,520,000
	UL.II	15,690,000	11,860,000	10,270,000	14,530,000	8,390,000	29,050,000
	UL.III	23,530,000	17,790,000	15,400,000	21,790,000	12,580,000	43,570,000

Source: outputs of OpRSA SW and author’s own elaboration. Figures in €

The Small and Medium Enterprises, Businesses and Professionals (SBP) of the mobile line segment estimated an average expected loss of 8 MM € in one year, and an average unexpected loss of 16 MM €; the rating classes defined the situation as manageable (62%) basically due to the event "suppliers, counterparties, contractors and other agents" which shows a critical rating. We found that the results indicated an unexpected loss higher that the expected loss (in every case except for the "fraud" event), which means a risk typology characterized by a medium-low frequency and a medium-high impact. This is reasonable for the relatively reduced number and size of customers compared to the Residential mobile line segment, and the high impact on them. As abovementioned, analyzing the event types, we found that only the event "suppliers, counterparties, contractors and other agents" obtained a critical classification of 63%, being "end customer", "poor quality" and "fraud and unauthorized activities" classified as acceptable.

The event "suppliers, counterparties, contractors and other agents" is the most significant, with an expected loss of 1,5 MM € and an unexpected loss of 10,8 MM €. The major contribution for this risk is "non-availability at source" with an expected loss of 1,4 MM € and an unexpected loss of 10,7 MM €; this event has a potentially catastrophic classification. The managers of this business unit argued that the main cause of this situation was the possibility of suppliers stopping offering the service, with real case examples of companies doing it.

In the case of the application of the OpRSA methodology to the Wholesale Business segment of the mobile line, the results are shown in Table 3.38.

Table 3.38. Results of Wholesale Business Segment of Mobile Line

EVENT TYPE		TYPE 1	TYPE 4	TYPE 5	TOTAL
		End Customer	Suppliers	Processes	
TOTAL	EL	30,000	160,000	190,000	380,000
	UL	260,000	640,000	540,000	1,440,000
	Rating A	**100.00%**	9.20%	**100.00%**	**100.00%**
	Rating B		83.60%		
	Rating C		7.20%		
	Rating D				
	UL.I	1,120,000	740,000	1,040,000	2,080,000
	UL.II	2,250,000	1,470,000	2,080,000	4,160,000
	UL.III	3,380,000	2,210,000	3,130,000	6,250,000

Source: outputs of OpRSA SW and author's own elaboration. Figures in €

The Wholesale Business segment of the mobile line, which is responsible for leasing networks to other telecommunications operators, estimated an average expected loss of 0,38 MM € in one year, and an average unexpected loss of 1,4 MM €; the rating classes were defined as acceptable which means an optimum situation with minimal risk of operating losses. The results showed an unexpected loss more than six times higher than the expected loss, so that the overall risk had a medium-low frequency and a medium-high impact. This is reasonable for the relatively reduced number and size of "customers" (other telecommunications companies), and the high impact on them. Analyzing the event types, we found that the event "suppliers, counterparties, contractors and other agents" obtained a manageable classification (83%), the rest of the events being an acceptable classification.

The main risk was "non-availability at source" with an expected loss of 0,16 MM € and an unexpected loss of 0,64 MM €. In accordance with the managers' comments, the main risk of this was losses due to delays of suppliers.

This quantitative data is the result of the application of the operational risk assessment methodology, and it was contrasted against the business unit managers, providing relevant information for the budgeting exercise across the company for the expected and unexpected losses, improving their decision making for capital allocation and, therefore, helping in cost reduction for the business unit.

3.3.2 Theoretical results

In order to give an appropriate interpretation of this research, it is important to summarize some key issues revealed by the literature review for connecting this paper's results to previous studies: (i) many companies belonging to various sectors still struggle with risk identification and evaluation techniques based on an ERM approach; (ii) in general, ERM have attracted little research attention compared to other disciplines; (iii) the risk management approach is in a state of maturity for financial firms, particularly in advanced techniques, methods and tools for operational risk assessment; (iv) operational risk evaluation for non-financial firms is not an easy practice; (v) there is a lack of research in ERM for non-financial companies, in particular for those in the telecommunications sector; (vi) ERM and its associated methodologies should be implemented in any type of organization, regardless of its sector, for creating value for its stakeholders; (vii) no practical risk evaluation methodology based on risk self-assessment and scenario analysis with the statistical and actuarial approach used in financial firms has been found and applied in the telecommunications sector; and (viii) the research based on case

studies has proven to be a best practice in ERM studies in order to build, contrast and illustrate ERM implementation results.

The results show that it is possible and useful to build practical risk identification frameworks and an assessment methodology (process and method) to help a telecommunications company (TELCO) in evaluating its operational risks, despite the abovementioned key aspects revealed by the literature review. In fact, the results of this research lead to a practical risk identification and evaluation approach for the business of a large company in contrast to other theoretical studies that are focused on the fundamentals of the ERM process. These studies do not provide a pragmatic and customized implementation of methodology and practices, even in different sectors or other types of organizations (Meidell and Kaarboe, 2017; Chen *et al.*, 2019). In fact, it has been relevant to review various studies on telecommunications companies. They are all mainly focused on empirical investigations about general characteristics of the sector due to globalization, which determines a continuous increase of risks for companies, particularly for large companies in a dynamic environment.

Another result of this study is the convergence between theoretical practices and those illustrated by TELCO's case study in building a practical management tool for supporting decision-making processes within a company. This is described, once the risks have been identified, in the OpRSA process phases and its embedded OpRSA method. In this respect, two innovative aspects resulting from this study are: (i) the use, enhancement and application of the conceptual COSO ERM framework for identifying and evaluating operational risks; and (ii) the extrapolation and adjustment of methods and techniques of common use in the financial sector to TELCO. These two aspects need to be put in the context that even though academics are increasingly examining the adoption and impact of ERM, their studies are commonly too general, inconsistent, and inconclusive due to an inadequate specification of how ERM is used in practice, applying specific methodology for its implementation (Mikes and Kaplan, 2013). This idea is extended to the creation and application of risk evaluation methodology and is due to the lack of knowledge of specific risk management techniques for large non-financial sectors such as telecommunications (Fraser and Simkins, 2016). For a large organization such as TELCO, it has been practical to organize regular workshops and questionnaires for data gathering and the risk self-assessment technique for the field work of the chosen business units, together with the key business representatives (managers). This approach was led and supported by senior management to ensure that the OpRSA process was conducted with rigor.

3.4 Empirical study conclusions

The main conclusion of the empirical study is the creation and analysis of the model's applicability to identify and evaluate operational risks for TELCO. Some reasons justify this assertion:

- It has been possible to obtain relevant information to develop the risk identification frameworks and the risk assessment methodology to create the operational risk identification and evaluation model for TELCO.
- The operational risk identification and evaluation model has produced consistent results with those expected, having been contrasted with the business units' managers within the research scope.
- The explanations and interpretations of the information collected in each of the tables of empirical results provide operational and business information for risk evaluation and undertake the next two phases of the risk management process (risk response, and monitoring and reporting). In fact, the interpretation of the tables of outputs (empirical results) include comments that, in addition to the numerical results of the risk estimation after having carried out the case study in TELCO, allow several conclusions to be deduced on certain decisions to be taken for the implementation of the model of identification and evaluation of its operational risks and their treatment.
- As explained above, one of the first decisions made in the case study was the level of the organizational structure to which the questionnaires would be addressed. The methodological option chosen, top-down and partial, has proved to be the most suitable for a company of the size and characteristics of TELCO, in terms of impact, time, effectiveness and in view of the results and information obtained.
- Another important aspect in the execution of the self-assessment process in TELCO has been implementing the questionnaires, i.e. the risks affecting each business unit. For this purpose, several meetings were held to prepare the execution of the questionnaire, as explained in the research design (sub-section 3.1).
- Regarding operational risk management, the proposed and applied model not only allows development of the risk control cycle (identification, prioritization, measurement and control of operational risks), but also for subsequent support in the management of these risks (action plans and risk treatment), as described below.

Concerning the link between the **propositions and the results** obtained in the empirical study, we can highlight the following:

- The results of the empirical study show that it has been possible to create frameworks for the identification of the main operational risks of TELCO, the case study of a large company in the telecommunications sector (**proposition 1**). Based on the research methodology tools for data gathering (mainly, brainstorming sessions and semi-structured interviews supported by questionnaires), we could identify the events (classified in 9 risk type groups), risk factors and risk effects frameworks (operational risk identification pillar) for TELCO. The information is detailed in the tables included in sub-section 3.2.1. These results were contrasted by TELCO managers, who finally confirmed its validity, both in terms of its structure and its specific content and examples evidencing the events.
- On the other hand, these empirical results show the development of a methodology for the evaluation of the operational risks identified for TELCO (**proposition 2**). Taking the identified risks as a starting point and applying the research methodology described, it was possible to develop the operational risk assessment process and method that make up the operational risk assessment methodology framework. This methodology was implemented for every organizational unit under the scope of the TELCO case study, where key managers were key informants for data collection. A quantitative analysis was performed of subjective estimates, the inputs of which were the economic impact and the probability of occurrence of every event for calculating expected, unexpected losses and rating classes for risk evaluation. The empirical results are shown in the tables included in sub-section 3.3.1. The numerical results, the interpretation of which is described, were analyzed jointly with TELCO managers to conclude that it was practical and adjusted information based on their experience on the measurement of each risk.
- Also, it is very useful information for decision-making regarding risk treatment and action plans. In fact, once TELCO's operational risk has been identified and measured, three main options can be considered for risk treatment (the option to avoid or terminate the risk has been omitted): mitigate the risks (mitigating actions), transfer them (e.g. insurance contracting) or accept them (include them in the annual budgets). This is described in the risk management process framework (sub-section 2.1.3). The explanation of these three options, based on a cost-benefit study to be carried out by managers, is the following:

- In terms of risk mitigation, the concepts used in this option are the following: expected losses (EL), unexpected losses (UL), Value at Risk (VaR)[14], Capital at Risk (CaR)[15], the cost of capital (WACC-Weighted Average Cost of Capital) and the cost of mitigating actions. Usually, the CaR is identified with the unexpected loss and the expected loss is included in the budget of the organizational unit. A mitigating action will have the effect of reducing both expected and unexpected losses. The decrease in expected losses represents a direct saving for the business unit, while the cost of capital must be taken into account to calculate the savings from the decrease in unexpected losses. Recall that the capital at risk represents the capital that the company must have to face unexpected losses due to operational risk. The results derived from the model implementation through the empirical study allow managers to consider the savings in capital cost due to unexpected losses and the savings in expected losses. In this case, the decision from a cost-benefit point of view would be to undertake the investment in the mitigating action.
- The decision to transfer risks consists mainly of taking out insurance. The concepts used in this option are the following: expected losses (EL), unexpected losses (UL), Value at Risk (VaR), Capital at Risk (CaR), cost of capital (WACC) and insurance premium. The insurance premium will have the effect of decreasing both expected losses and unexpected losses. The decrease in expected losses represents a direct saving for the business unit, while the cost of capital must be considered to calculate the savings from the decrease in unexpected losses. Recall that the capital at risk represents the capital that the company must have to face unexpected losses due to operational risk. The calculation will be analogous to the previous one, with the difference that the insurance premium is also annual. Once the measurement has been made, the causes (factors) have been

[14] VAR is defined as the sum of expected loss and unexpected loss, reflecting the maximum expected loss during a time interval, in this case 1 year, with a confidence level of 99.9%.

[15] CAR is identified with the portion of the value at risk not included in the ordinary activity and therefore outside the scope of budgeting.

identified, the possible mitigating or risk transfer actions have been analyzed (by means of an analysis), TELCO may choose to assume the risk. Considering that the expected loss (EL) is included in the ordinary activity of the company, the unexpected losses (UL) define the capital that the company must have available to face the operational risk, known as Capital at Risk (CAR).

- The third option, once the measurement has been carried out, the causes (factors) have been identified, the possible mitigating or risk transfer actions have been analyzed (through the cost-benefit analysis), TELCO can choose to assume the risk. Considering that the expected loss (EL) is included in the company's ordinary activity, the unexpected losses (UL) define the capital that the company must have available to face the operational risk, known as Capital at Risk (CAR).

In short, the most relevant conclusion of the empirical study is that it has been possible to contrast the specific propositions of the research, linking the data to the research propositions. The criteria for the interpretation of the findings are contained in the creation of the model itself, both for TELCO's events identified and the operational risk assessment methodology. Also, the verification of these propositions responds to the research objectives and associated questions.

4 CONCLUSIONS

4.1 Main findings

There is a general consensus that the growth in popularity of enterprise risk management's (ERM) frameworks has resulted from a response to requirements on organizations to manage risk. However, several ERM studies (Lundqvist, 2014) question the validity of these models, arguing that being accepted in the communities which study risk management, they may turn out to be theoretical and general models to have a successful practical application in the companies. This limitation is even bigger in respect of the challenge of identifying and evaluating operational risks for a large telecommunication company, where there is a lack of contrasted references versus all the assessment models implemented in the banking sector (BCBS, 2006; Dutta and Perry, 2006; Fontnouvelle and De Jesús, 2003; Singh and Hong, 2020). This study attempted to examine how telecommunications companies can identify and evaluate

their operational risks based on a case study. The operational risk identification and evaluation model presents relevant frameworks, process and method, including the steps that practitioners can find useful and meaningful for telecommunications firms. Furthermore, the proposed model and its results, the main contribution of this research, were empirically validated with TELCO's managers and showed high levels of reliability and validity. This study highlights that in a dynamic and complex world of business, ERM frameworks can be customized for firm needs, in particular for managing their operational risks for enhancing performance and value creation. McShane (2018) argues that "even with two prominent ERM frameworks (COSO ERM and ISO 31000), organizational contexts make a one-size-fits-all method of implementing ERM impossible", and this is the basic reason for research in creating innovative risk identification frameworks (OpRIF) and similar evaluation methodologies such as OpRAM (operational risk assessment methodology).

Advancement of ERM research has been hampered by a complex evolution involving competing associations, frameworks and standards. This is particularly clear in the case of applying practical methods for risk identification and evaluation. This study moves beyond the limited potential of theoretical approaches through qualitative and quantitative analysis by conducting a field study for a business case in order to understand what telecommunications companies might do for implementing ERM processes, where risk identification and evaluation are the critical steps. Over the previous few decades, various risk management approaches have been described by accounting scholars that do not yield to disciplinary solutions. Much of the academic work on ERM comes from finance, while complex firms' environment cannot be effectively handled by a single discipline or knowledge of one specific sector. Interdisciplinary efforts are required for the ERM philosophy to become effective, and this is the reason by which collaboration from multiple disciplines is essential for the advancement of ERM strategies (McShane, 2018), as well as for research such as that proposed in this study.

In summary, the **main findings** of this technology transfer research include:

- The ERM studies of some organizations reveal their limited impact on the results of their operations, as they are considered too generic and theoretical. In fact, based on the literature reviewed, there are currently no practical and proven references to the application of management models for the identification and assessment (evaluation) of operational risks in the telecommunications sector;
- The creation of a simplified and easy-to-understand risk management process based on the most recognized standards and frameworks in the risk discipline for the

selection of the two most important phases of this process and its risk category: the identification and evaluation of operational risks;

- The identification of operational events, risk factors and effects based on the TELCO case study;
- The development of an operational risk evaluation methodology for evaluating operational risks, based on the TELCO case study, based on a risk self-assessment process and method;
- As part of the research design, the methodology and techniques used for the empirical study, as well as the telecommunications company selected as a business case, have yielded empirical and conceptual results that corroborate, confirm, validate and support the main proposition and objectives of this study.
- It is definitely feasible, relevant, practical and useful for different groups (e.g. directors, executives, practitioners, researchers, professionals, and the academy and organizations, in general) to identify an operational risk identification and evaluation model applied to the telecommunications sector, based on its application to a company case (TELCO) and extrapolated to other companies in the same sector, and even to other types of industries; and finally,
- The findings of this research study reveal the contributions, practical implications, future research and limitations, as well as the lessons learned, requirements, and key success factors for designing and implementing an operational risk identification and evaluation model in a telecommunications company.

4.2 Contributions and implications

4.2.1 Main contributions

The analysis of the results provides a significant understanding of the proposed operational risk identification and evaluation model and its practical application, and therefore offers several theoretical and managerial contributions and practical implications.

The research adds to our theoretical understanding of the topic (ERM) at several levels. First, the study proposes an innovative operational risk identification and evaluation model based on universally-accepted ERM frameworks. Second, regarding risk evaluation, the research considers operational risks proven and robust experiences from the financial and insurance sector (e.g. loss distribution approach, actuarial approach). Third, as the risk identification and evaluation steps are key in the risk management

process, the research provides a practical approach for ERM implementation based on the theoretical concepts included in the various risk management standards and frameworks. In this sense, the contribution of this work is based on the effective creation (building) and application of an operational risk identification and evaluation model for TELCO which would allow the establishment, as a “best practice”, of the implementation of operational risk management models, entirely aligned with commonly accepted frameworks (COSO) and standards (ISO 31000) on this subject. Fourth, once TELCO already has historical data as a result of this research, the operational risk identification and evaluation model developed in this study would facilitate development of a loss event data capture process (LDC) which should be capable of identifying, validating and obtaining results on operational losses in a reliable manner, ensuring: (i) integrity of the data recorded; (ii) accessibility of the information recorded; and (iii) the quality and quantity of the information recorded.

The research also has several managerial contributions. First, as organizations have to focus on developing risk management practices to identify and evaluate their operational risks, the proposed model is a practical approach to achieve it for the telecommunications industry where there is a lack of literature and research. Second, companies from other sectors, apart from financial, insurance, and TELCOs, can extrapolate the content of this research for identifying and measuring their operational risks using robust and contrasted risk identification frameworks and risk evaluation methodology (process and method). Third, the results imply that there is a strong and direct impact of risk management practices on firm performance, as the operational risk which can be identified and evaluated, are key for the business. Fourth, regarding the LDC process based on the development of the operational risk identification and evaluation model, it would contribute in the: (i) creation of a solid culture in the organization by means of involving the all the business units in the LDC process and defining and disseminating a single common recording methodology; (ii) formalization of the LDC process (identification, validation and reporting); and (iii) implementation of a dynamic process that can update information sources and accurately reflect the company’s exposure to operational risks according to the organization’s evolution. Fifth, the study can be appreciated by managers for contrasting their previous knowledge about operational risk impact; in fact, outstanding organizations focus on learning from failures and improving organizational processes for risk prevention in the future, and better responsiveness performance in the present, where this risk identification and evaluation model can be a relevant “management tool” for the decision-making process.

4.2.2 Practical implications

Furthermore, there is a two-fold set of practical implications: business implications and implications for researchers and practitioners. Regarding business implications, the results of the application of the risk identification and evaluation model were contrasted with TELCO's business managers who confirmed their reliability and usefulness for their decision-making processes. This research work would help TELCO companies to understand the usefulness and applicability of the proposed model to provide value for their stakeholders for: (i) obtaining relevant information to allow management to effectively assess overall capital needs; (ii) reducing operational surprises and losses and improving risk response decisions; (iii) managing multiple and cross-enterprise risks, considering a full range of potential events, in order to realize business opportunities; and (iv) aligning risk appetite and strategy. The Milliman Risk Institute, in 2014, performed a survey-based study that indicated the top five ways ERM creates value for firms, including improved performance management, enhanced board oversight, higher quality of strategic planning, improved risk-adjusted decision making, and improved capital efficiencies (allocation). The last two ways have been covered by this study by efficiently identifying and evaluating the operational risks in a TELCO. Additional practical implications of this study are linked to some benefits of a sound ERM framework and the fact that risk managers should refrain from only focusing on theoretical models but strive to produce risk identification and evaluation that can be practical for decision-making to identify concrete outcomes. The business units and risk owners should gain from having a comprehensive view of risks, as well as analyzing the risk profile of their activity under adverse conditions. The risk discipline and risk culture can be promoted by an active risk management contribution (Fiol, 2019). Furthermore, the implementation of risk management models for companies in the telecommunications sector results in the improvement of decision-making processes on risks, it enables control activities, it contributes to efficient allocation of the company's capital and funds, and it protects and increases the company's property. Balancing between the benefit that a certain method brings and the costs it creates is the basic criterion for the application of risk management frameworks in companies in the telecommunications sector. In some cases, external influence, such as state regulations, can affect the selection of the method to be applied in risk management.

Regarding the implications for researchers and practitioners, this study for evaluating operational risks might be used as a benchmarking tool for other entities and industrial sectors, not only for practitioners but also for researchers. Researchers following the

path described in this study might be interested in proposing similar risk identification frameworks (OpRIF) and OpRAM methodology for the application in other industries and develop business cases to illustrate the usefulness of the approach. Bromiley et al. (2015) provides a critical review of ERM research for identifying limitations and gaps that management scholars are best equipped to address, including the need for management research for ERM development. Their study contributes with relevant insights for identification and measurement of risks in ERM, analyzing concepts such as how managers assessments of risk may differ from objective measures of risk, as individuals at the top of firms probably have greater confidence in their judgments than the normal individual, being more experienced managers for the risk management process. Finally, this research could also contribute to the academic community in consolidating theoretical concepts and a practical approach for the ERM discipline.

4.3 Further implications

4.3.1 Future lines of research

For future research directions, this study provides an initial foundation that can spawn additional research on operational risk identification and evaluation. First, researchers should be encouraged to examine other TELCOs' approaches to ERM, as well as to explore other sectors, as the methodology could be extrapolated to them. I believe that the academic community is positioned to greatly contribute to this growing risk management policy need for more effective ERM in multiple sectors. As far as it has been analyzed and based on the literature review of ERM, this study could be considered as an innovative research study to explore a practical model for operational risk evaluation in a large TELCO, as well as a good reference for further research, not only in the telecommunications sector, but also in other industries in addition to finance and insurance. Therefore, future studies could conduct an in-depth case study of additional firms in every sector (Singh and Hong, 2020). Second, future research could consider not only the operational risks identified in the operational risk identification methodology, but also those included in a broader classification such as the one described in Figure 2.3. Third, future research could cover the two final steps of the risk management process (i.e. risk response and risk monitoring and reporting), considering that risk treatment and ways of reporting may differ from one firm to another depending on their risk appetite, and for this reason results should be focused on specific companies, difficult to extrapolate on other companies in the same or different sectors. Fourth, future research may also revisit the cultural factor of attention to detail. This may be because ERM maturity is not good enough yet and attention is mainly focused on documents and

standard operating procedures, more than customized methodologies for firms, which may have adverse consequences for the effective implementation of risk management practices. Fifth, extrapolation of this research to other industries could be useful and efficient for other firms in order to enhance their performance. Finally, other proposals for further research could include the ERM relationship with related disciplines such as business sustainability, corporate governance, corporate social responsibility, and compliance.

4.3.2 Limitations

Limitations in this research approach are also acknowledged. First, due to the dimension and scope of TELCO, the field work had to be limited to two specific business units, while the exploration of a bigger sample could have provided additional and richer results about the validity of the results. Second, it is uncertain that a similar research study could be performed and tested in any other telecommunications company without an ERM strategy in place. An ERM program for identifying and evaluating risks must have an organizational mandate to be implemented effectively and have the right people in place to identify, measure and manage the risks of the firm. In this sense, we used survey data (questionnaires) obtained from the managers. To the extent that those executives might not have accurate first-hand knowledge about the risks to be identified and evaluated within their business units, the research results could be biased, limiting our ability to find inputs consistent with the business results. This situation could be minimized and enhanced based on the authority, knowledge and experience of the interviewees (managers), as was done and double-checked along the study. Third, other statistical approaches and distributions in the OpRSA method could contribute with different and unexpected results. Fourth, the case study is mainly based on primary data (the information collected and recorded directly from the respondents, the managers and subject matter experts), while the use of secondary data compiled inside and outside of the company is limited due to the lack of risk registers repository; only annual and internal reports from the company were available for this new risk management approach. Finally, one relevant limitation is that various previous studies have relied on the practice of Chief Risk Officer (CRO) appointments as a proxy for risk management and evaluation (Beasley et al., 2008; Hoyt and Liebenberg, 2011; Pagach and Warr, 2011), and the results of the research could not be contrasted with this non-existent function in TELCO at the time of the study.

4.3.3 Managerial implications

Finally, some implications from the research applied to the TELCO case study include the following: (i) the operational risk management implementation is a complex process and it is important to make it as easy as possible in order to avoid change resistance. Over time, more sophisticated measures can be deployed, once the managers buy-in insight is completed due to the importance of risk management for the organization; (ii) the quality of the key information is much more important than the quantity; (iii) risk management reports should be available for decision-makers, with formalized information flows, and effective reporting facilitates proactive operational risk management with clear messages to the organization; (iv) the objective of the reporting process is not only the risk evaluation but also the implementation of the rest of the components of the risk management process such as the risk treatment and implementation and mitigating plans; (v) the practical know-how related to risks matters which is already available in TELCO (even being incomplete) is relevant for the operational risk identification and evaluation model, considering the interactive approach with managers for data gathering; and (vi) events and risk factor owners need to be supported by the management team and middle-managers in order to interpret the results appropriately.

In relation to the lessons learned, from a professional practice point of view, for the effective implementation of an operational risk identification and evaluation model in a company of the scope and size of TELCO, such as the one studied in this research, a set of requirements, key success factors, as well as an understanding of the main reasons why the implementation of a model such as the one proposed could not work well enough, should be considered.

For the effective implementation of an operational risk identification and evaluation model, the following requirements should be considered: (i) a risk management policy supported by the management team; stakeholder focus and leader involvement are required for interest on cultural change; (ii) risk management procedures where the proposed model is part of them; (iii) a risk management organizational structure with “subject matter experts” with the necessary competences to deal with and resolve risk matters; and with knowledge of operational risk management techniques; as well as (iv) a risk management system or tool for the administration of the proposed model.

In addition, and with the same objective of making the implementation of the operational risk identification and evaluation model effective and useful, the following key success factors should be considered: (i) set the “tone” and culture for managing and embedding risks, as well as for creating a “common language” for risk management and for identifying coherent objectives for motivating the organization; (ii) identify “stakeholders” for supporting the “new model” for identifying and evaluating operational risks, as well as defining roles and responsibilities, guaranteeing an appropriate escalation process, for the effective implementation of the model; (iii) ensure the homogenization and organization of rules, policies, management, risk control and assessment methodologies, as defined in the model; and (iv) revise periodically the effectiveness and adequacy of the operational risk identification and evaluation model.

Furthermore, the main reasons why the operational risk management and identification could not work as expected are: (i) internal focus only, meaning that no benchmarking activities are performed by the organization to identify best practices on implementation of risk management models; (ii) unnecessary bureaucracy and delegation of responsibilities on risk management to standards and specialists; (iii) not having an open mind to be willing to change the organization as a result of the implementation of the new model, not encouraging such initiative, as well as implementing the model only partially in the company, not from beginning to end (end-to-end); and finally (iv) not having internalized the importance of implementing such a model, with the benefits it entails.

A final “food for thought” comment, as a personal opinion, is that research in risk management in telecommunications and information technology companies is a worth-while “investment”, as the activities of these sectors stipulate the functioning of not only the entire social system needs, but also the life of the contemporary individual, improving the welfare state.

5 REFERENCES

Aabo, T., Fraser, J.R.S., & Simkins, B.J. (2005). The rise and evolution of the chief risk officer: enterprise risk management at Hydro One. *Journal of Applied Corporate Finance,* 17(3), 62-75, 689-698.

Abkowitz, M.D. (2008). *Operational risk management. A case study approach to effective planning and response*. NJ: John Wiley & Sons.

Anomaly, J., & Brennan, G. (2014). Social norms. The invisible hand, and the law. *University of Queensland Law Journal*, 33(2).

Altuntas, M., Berry-Stölzle, T.R., & Hoyt, R.E. (2020). Enterprise risk management adoption and managerial incentives. *Journal of Insurance Issues*, 43(2), 1-42.

Anton, S.G. (2018). The impact of enterprise risk management on firm value: Empirical Evidence from Romanian Non-Financial Firms. *Inzinerine Ekonomika-Engineering Economis*, 29(2), 151-157.

Arena, M., Arnaboldi, M., & Azzone, G. (2010). The organizational dynamics of enterprise risk management. *Journal of Accounting, Organizations and Society*, 35, 659-675.

Armstrong, C. S., Guay, W.R., Mehran, H., & Weber, J.P. (2016). The role of financial reporting transparency in corporate governance. *Economic Policy Review*, 107-128 (August).

Ashby, S. (2008). Operational risk: Lessons from non-financial organisations. *Journal of Risk Management in Financial Institutions*, 1(4), 406-415.

Barlow, D. (1993). The evolution of risk management. *Risk Management*, 40(4), 38.

Barton, T., Shenkir, W.G., & Walker, P.L. (2002). *Making enterprise risk management pay off*. NJ: Financial Times Prentice Hall.

Barton, T., Shenkir, W.G., & Walker, P.L. (2012). Enterprise risk management: skipping the ERM tune-up: pay now or pay later. *Financial Executive Magazine*, 28(10), 22-25.

Basel Committee on Banking Supervision. (2002). *Operational risk data collection exercise*. Basel I Accord-Standards. Bank of International Settlements. Basel: BCBS.

Basel Committee on Banking Supervision. (2003). *Sound practices for the management and supervision of operational risk*. Basel I Accord-Standards. Bank of International Settlements. Basel: BCBS.

Basel Committee on Banking Supervision. (2004). *International convergence of capital measurement and capital standards: A Revised Framework*. Basel II Accord-Standards. Basel: BCBS.

Basel Committee on Banking Supervision. (2006). *International convergence of capital measurement and capital standards: a revised framework*. Basel II Accord-Standards. Bank of International Settlements. Basel: BCBS.

Basel Committee on Banking Supervision. (2008). *International convergence of capital measurement and capital standards: a revised framework*. Basel II Accord-Standards. Bank of International Settlements. Basel: BCBS.

Basel Committee on Banking Supervision. (2009). *Enhancements to the Basel II framework. Basel II Accord-Standards*. Bank of International Settlements. Basel: BCBS.

Basel Committee on Banking Supervision. (2011). *A global regulatory framework for more resilient banks and banking systems*. Bank of International Settlements. In: Basel III Accord-Standards. Basel: BCBS.

Baxter, R., Bedard, J.C., Hoitash, R., & Yezegel, A. (2013). Enterprise risk management program quality: determinants, value relevance, and the financial crisis. *Contemporary Accounting Research*, 30(4), 1264-1295.

Beals, S., Fox, C., & and Minsky, S. (2015). Why a mature ERM effort is worth the investment. *The Risk Perspective Executive Report*. NY: Risk Insurance and Management Society (RIMS).

Beasley, M. S., Clune, R. and Hermanson, D.R. (2005). Enterprise risk management: an empirical analysis of factors associated with the extent of implementation. *Journal of Accounting and Public Policy*, 24(6), 521-531.

Beasley, M. S., Donald P. Pagach, D.P., & Warr, R.S. (2008). Information conveyed in hiring announcements of senior executives overseeing enterprise-wide risk management processes. *Journal of Accounting Auditing Finance*, 23(3), 311-332.

Bedford, T., & Cooke, R. (2001). *Probabilistic risk analysis: foundations and methods.* Cambridge: Cambridge University Press.

Bernstein, P.L. (1998). *Against the Gods. The remarkable story of risk*. NY: John Wiley & Sons.

Bertinetti, G. S., Cavezzali, E., & Gardenal, G. (2013). *The effect of enterprise risk management on firm value of European companies*. Working Paper No. 10. Venice: Università Ca' Foscari Venezia. Department of Management.

Bharathy, G., & McShane, M. (2014). Applying a systems model to enterprise risk management. *Engineering Management Journal*, 26(4), 38-46.

Blanco-Mesa, F., Rivera-Rubiano, J., Patiño-Hernández, X. & Martínez-Montaña, M. (2019). The importance of enterprise risk management in large companies in Colombia. *Technological and Economic Development of Economy Journal*, 25, 600-633.

Breden, D. (2008). Monitoring the operational risk environment effectively. *Journal of Risk Management in Financial Institutions*, 1(2), 156-164.

British Standards Institution. (2007). Draft BSI 31100. *Code of practice for risk management*. London: BSI.

Bromiley, P., McShane, M., Nair, A., & Rustambekov, E. (2015). Enterprise risk management: review, critique, and research directions. *Long Range Planning Journal*, 48, 265-276.

Brown, J., Duane, M., & Schuermann, T. (2019). What is enterprise risk management? *Journal of Risk Management in Financial Institutions*, 12(4), 311-319.

Cadbury (1992). *The financial aspects of corporate governance*. The Committee on the Financial Aspects of Corporate Governance. London: Gee-Professional Publishing.

Callahan, C., & Soileau, J. (2017). Does Enterprise risk management enhance operating performance? *Advances in Accounting*, 37, 122-39.

Cendrowski, H., & Mair, W.C. (2009). *Enterprise risk management and COSO. A guide for directors, executives and practitioners*. NJ: John Wiley & Sons.

Chance, D. M., & Brooks, R. (2010). *An introduction to derivates and risk management*. Boston: Cengage Learning.

Chapman, R.J. (2008). *Simple tools and techniques for enterprise risk management*. NY: John Wiley & Sons.

Chen, J., Jiao, L., & Harrison, G. (2019). Organisational culture and enterprise risk management: The Australian not-for-profit context. *Australian Journal of Public Administration*, 78(3), 432-448.

Chermack, T.J. (2011). *Scenario planning in organizations: how to create, use, and assess scenarios*. Colorado: Berret-Koehler.

Chernobai, A. S., Rachev, S.T., & Fabozzi, F.J. (2007). *Operational Risk: A Guide to Basel II Capital Requirements, Models, and Analysis, XV-XVI*. NJ: John Wiley & Sons.

Chew, D.H. (2008). *Corporate risk management*. NY: Columbia University Press.

Ching, H. Y., & Colombo, T.M. (2015). Enterprise risk management good practices and proposal of conceptual framework. *Journal of Management Research*, 6(3), 69-85.

Cohen, A.V. (1996). Quantitative risk assessment and decisions about risks: an essential input into the decision process. In *Accident and design: Contemporary Debates in Risk Management* (pp. 87-98). London: UCL Press.

Comisión Nacional del Mercado de Valores [Nacional Stock Marquet Comisión]. (2015). *Good governance code of listed companies*. Madrid: CNMV.

Committee of Sponsoring Organizations of the Treadway Commission. (1992). *Internal control. Integrated framework*. NY: COSO.

Committee of Sponsoring Organizations of the Treadway Commission. (2004). *Enterprise risk management. Integrated framework*. NY: COSO.

Committee of Sponsoring Organizations of the Treadway Commission. (2004). *Enterprise risk management. Integrated framework. Application techniques*. NY: COSO.

Committee of Sponsoring Organizations of the Treadway Commission. (2004). *Enterprise risk management. Integrated framework*. Executive summary framework. NY: COSO.

Committee of Sponsoring Organizations of the Treadway Commission. (2013). *Internal control. Integrated framework*. NY: COSO.

Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Enterprise risk management. Integrating with strategy and performance*. NY: COSO.

Conthe (2006). *Unified good governance code of listed companies*. Comisión Nacional del Mercado de Valores (CNMV) [National Stock Market Commission]. Madrid: CNMV.

Coromina, E., Casacubierta, X., & Quintana, D. (2002). *El trabajo de investigación. El proceso de elaboración, la memoria escrita y los recursos*. Barcelona: Eumo-Octaedro.

Crouhy, M., Galai, D., & Mark, R. (2006). *The essentials of risk management*. NY: McGraw-Hill.

Cruz, M.G. (2005). *Modelling, measuring and hedging operational risk*. London: John Wiley & Sons.

Damodaran, A.. (2008). *Strategic risk taking. A framework for risk management*. NJ: Wharton School Publishing.

D'Arcy, S.P., & Brogan, J.C. (2001). Enterprise risk management. *Journal of Risk Management of Korea*, 12(1), 207-228.

Delbecq, A.L. (1968). The world within the span of control. Managerial behaviour in groups of varied size. *Business Horizons Journal*, 11(4), 47-56.

Deloach, J. (2000). *Enterprise-wide risk management: strategies for linking risk and opportunity.* London: Financial Times/Prentice-Hall.

Deloitte. (2020). *A moving target: refocusing risk and resiliency amidst continued uncertainty by Caldwell, J.H*. London: Deloitte & Touche LLP.

De Lima, M.L. (2004). Images on the public in the debated about risk. Consequences for participation. *Portuguese Journal of Social Science*, 2(3), 149-163.

Dias, A.P. (2017). A more effective audit after COSO ERM 2017 or after ISO 31000:2009? *Perspectiva Empresarial [Business Perspective]* 4(2), 73-82.

Dickinson, G. (2001). Enterprise risk management: its origins and conceptual foundation. *The Geneva Papers on Risk and Insurance*, 26(3), 360-366.

Dickstein, D.I., & Flast, R.H. (2009). No excuses. *A business process approach to managing operational risk*. NJ: John Wiley & Sons.

Diebold, F.X., Schuermann, T., & Stroughair, J.D. (2000). Pitfalls and opportunities in the use of extreme value theory in risk management. *The Journal of Risk Finance*, 1(2), 30-36.

Donaldson, P. (1995). The stakeholder theory of the corporation: concepts, evidence, and implications. *Academy of Management Review*, 20(1), 65-91.

Dos Santos, M. P. F., Clarke, W.A., & Nel, A.L. (2005). *Enhancing Telecommunications Business Operations by Implementing Operational Risk Management in Service Level Management Operations*. TeleManagement Forum, eTOM the Business Process Framework-For the Information and Communications Services Industry. Johannesburg: Faculty of Engineering South Africa.

Dutta, K., & Perry, J. (2006). *A tale of tails: an empirical analysis of loss distribution models for estimating operational risk capital*. Boston: Federal Reserve Bank of Boston.

Eisenhardt, K.M. (1998). Building theories from case study research. *Academy of Management Review*, 14(4), 532-550.

Eisenhardt, K.M., & Brown, S.L. (1998). Competing on the edge. Strategy as structured chaos. *Long Range Planning*, 31(5), 786-789.

Elliot, M. (2013). *Enterprise risk management*. American Institute for Chartered Property Casualty Underwriters, Pennsylvania: AICPCU.

Embrechts, P., Klueppelberg, C., & Mikosch, T. (1997). *Modelling extremal events*. Applications of Mathematics No. 36. Berlin: Springer.

Espiñeira, Sheldon & Asociados. (2008). *COSO y el marco de gestión Integral de Riesgos*. Caracas: PricewaterhouseCoopers (PwC).

EURELECTRIC (2007). *Risk Management in the electricity industry-white paper I-overall perspective*. Brussel: Group of Risk Management-UNION OF ELECTRICITY INDUSTRY.

EURELECTRIC (2007). *The role of electricity. White paper for corporate operational risk management*. Brussel: Group of Risk Management-UNION OF ELECTRICITY INDUSTRY.

European Foundation for Quality Management. (2005). *The EFQM framework for risk management. Driving Excellence in Risk Management*. Brussels: EFQM-DNV.

European Foundation for Quality Management. (2019). *The EFQM model*. Brussels: EFQM.

Ernst and Young. (2020). *Top 10 risks in telecommunications 2020*. London: Ernst & Young (EY).

Fiol, F. (2019). Enterprise risk management: towards a comprehensive yet practical enterprise risk function. *Journal of Risk Management in Financial Institutions*, 12(4), 320-327.

Florio, C., & Leoni, G. (2017). Enterprise risk management and firm performance: the Italian case. *The British Accounting Review*, 49(1), 56-74.

Fontnouvelle, P., & De Jesús, V. (2003). *Using loss data to quantify operational risk*. Boston: Federal Reserve Bank of Boston.

Forcadell, F.J., & Aracil, E. (2019). Can multinational companies foster institutional change and sustainable development in emerging countries? A case study. *Business Strategy and Development Journal*, 2, 91-105.

Forester, J., Kolaczkowski, A., Lois, E., & Kelly, D. (2006). *Evaluation of human reliability analysis methods against good practices*. NUREG-1842 Final Report. Washington: U.S. Nuclear Regulatory Commission.

Foto, G., Manoku, E., & Sinaj, V. (2018). *Risk management in the telecommunication Industry. Case Study AMC*. In Konferenca e Katërt Ndërkombëtare për Riskum [Fourth International Conference for Risks]–QSHR [Albanian Center for Risks], Conference Paper. Tirana: Faculty of Economy, Tirana University, pp. 203-212.

Fraser, J.R.S, & Simkins, B.J. (2008). Ten common misconceptions about enterprise risk management. *Harvard Business Review*, 84, 36-48.

Fraser, J.R.S., Schoening-Thiessen, K., & Simkins, B.J. (2008). Who reads what most often? A survey of enterprise risk management literature read by risk executives. *Journal of Applied Finance*, 18(1), 73-91.

Fraser, J.R.S. (2010). How to prepare a risk profile. In *Enterprise risk management: today's leading research and best practices for tomorrow's executives* (pp. 171-188). NJ: John Wiley & Sons.

Fraser, J.R.S., Simkins, B.J., & Narvaez, K. (2014). *Implementing enterprise risk management: case studies and best practices*. NJ: John Wiley & Sons.

Fraser, J.R.S., & Simkins, B.J. (2016). The challenges and solutions for implementing enterprise risk management. *Elsevier Business Horizons Journal*, 59, 689-698.

Gandini, G., Bosetti, L., & Almici, A. (2014). Risk management and sustainable development of telecommunications companies. *Emerging Issues in Management (Symphoya)* 2, 1-14.

Garvey, P.R., Book, S.A., & Covert, R.P. (2016). *Probability methods for cost uncertainty analysis: a systems engineering perspective*. NY: Chapman and Hall/CRC Press.

Gatzert, N., & Martin, M. (2015). Determinants and value of enterprise risk management: empirical evidence from the literature. *Risk Management and Insurance Review*,18.

Gill, J., & Johnson, P. (2010). *Research Methods for Managers*. CA: SAGE Publications.

Gjerdrum, D., & Peter, M. (2011). The new international standard on the practice of risk management – a comparison of ISO 31000:2009 and the COSO ERM framework. *Risk Management Journal*. Canadian Institute of Actuaries. Casualty Actuarial Society. Society of Actuaries, 21, 8-12.

Goldenberg, O., & Wiley, J. (2011). Quality, conformity and conflict: questioning the assumptions of Osborn's brainstorming technique. *Journal of Problem Solving*, 3(2), 96-118.

Gordon, L.A., Loeb, M.P., & Tseng, C-Y. (2009). Enterprise risk management and firm performance: a contingency perspective. *Journal of Accounting and Public Policy* 28, 301-327.

Grody, A.D., Harmantzis, F.C., & Kaple, G.J. (2006). Operational risk and reference data: exploring costs, capital requirements and risk mitigation. *Journal of Operational Risk*, 1 (3).

Guba, Y., & Lincoln, E. (1985). *Publications. Naturalistic Inquiry*. CA: SAGE.

Guillen, M., Gustafsson, J., Nielsen, J.P., & Pritchard, P. (2007). Using external data in operational risk. *The Geneva Papers*, 32, 178-189.

Hampel (1998). Committee on corporate governance. The Committee on Corporate Governance. London: The Hampel Committee.

Hargreaves, J. (2010). Quantitative risk assessment in ERM. How to prepare a risk profile. In *Enterprise risk management: today's leading research and best practices for tomorrow's executives* pp. (219–235). NJ: John Wiley & Sons.

Harrell, M.C., & Bradley, M.A. (2009). *Data collection methods – A training manual – a Semi-structured interviews and focus groups*. CA: RAND Corporation. National Defense Research Institute.

Hopkin, P. (2002). *Holistic risk management in practice*. London: Kogan Page.

Hopkin, P. (2010). *Fundamentals of risk management. Understanding, evaluating and implementing effective risk management*. London: Kogan Page.

Hoyt, R. E., & Liebenberg, A.P. (2011). The value of enterprise risk management. *Journal of Risk and Insurance*, 78(4), 795-822.

Hoyt, R. E., & Liebenberg, A.P. (2015). Evidence of the value of enterprise risk management. *Journal of Applied Corporate Finance* 27(1), 41-47.

Hubbard, L. (2005). *Control Self-Assessment: a practical guide*. FL: IIA (The Institute of Internal Auditors).

Huber, M., & Rothstein, H. (2013). The risk organization: or how organisations reconcile themselves to failure. *Journal of Risk Research*, 16(6), 651-675.

Hughes, L.C., & Preski, S. (1997). Using key informant methods in organizational survey research: Assessing for informant bias. *Research in Nursing and Health*, 20(1), 81-92.

Ibrahim, F.S., & Esa, M. (2017). A study on enterprise risk management and organizational performance: developer's perspective. *International Journal of Civil Engineering and Technology (IJCIT)*, 8,184-196.

Instituto de Auditores Internos. (2006). *Marco para la práctica profesional de la auditoría interna*. Madrid: IAI.

Institute of Internal Auditors. (2004). *The professional practices framework*. FL: IIA.

Institute of Internal Auditors. (2009). *IIA position paper: the role of internal auditing in enterprise-wide risk management*. FL: IIA.

Institute of Internal Auditors. (2020). *Risk in focus 2021. Hot topics for internal auditors*. FL: IIA.

International Organization for Standardization. (2009). *Risk management. Principles and guidelines*. ISO 31000. Geneve: ISO.

International Organization for Standardization. (2009). *Risk management. Vocabulary. ISO Guide 73*. Geneve: ISO.

International Organization for Standardization. (2015). *Quality management systems. Requirements*. ISO 9001. Geneve: ISO.

International Organization for Standardization. (2018). *Risk management. Guidelines*. ISO 31000. Geneve: ISO.

International Organization for Standardization/International Electrotechnical Commission. (2008). *Uncertainty of measurement. Part 3: Guide to the expression of uncertainty in measurement (GUM: 1995). Supplement 1: propagation of distributions using Monte Carlo method*. ISO/IEC Guide 98-3. Geneve: ISO/IEC.

International Organization for Standardization/International Electrotechnical Commission. (2009). *Risk management. Risk assessment techniques*. ISO/IEC 31010. Geneve: ISO/IEC.

International Organization for Standardization/International Electrotechnical Commission. (2019). *Risk management. Risk assessment techniques*. ISO/IEC 31010. Geneve: ISO/IEC.

IRM. (2002). A risk management standard. Institute of Risk Management. London: IRM (Institute of Risk Management). AIRMIC (The Association of Insurance and Risk Manager). ALARM (The Public Risk Management Association).

Jacobus, D. (2015). New paradigm of managing risks: risk and control self-assessment. In *The 2014 International Conference on Agro-industry (ICoA): competitive and sustainable Agro-industry for Human Welfare*. Agriculture and Agricultural Science Procedia, 3, (pp. 32-34).

Jobst, A. (2007). It's all in data-consistent operational risk measurement and regulation. *Journal of Financial Regulation and Compliance*, 15(4), 423-449.

Jordan, S., Jorgensen, L., & Mitterhofer, H. (2013). Performing risk and the project: risk maps as mediating instruments. Management Accounting Research, 24(2), 156-174.

Karaca, S.S., & Senol, Z. (2017). The Effect of Enterprise Risk Management on Firm Performance: A Case Study on Turkey. *Studii Finaciare [Financial Studies]*, 21(2), 6-30.

Karanja, E. (2016). Does the hiring of chief risk officers align with the COSO/ISO enterprise risk management frameworks? *Journal of Accounting and Information Management*, 25(3), 274-295.

Kates, R.W. (1985). *Hazard assessment: art, science, and ideology*. NJ: Westview Press.

Kleffner, A.E., Lee, R.B., & and McGannon, B. (2003). The effect of corporate governance on the use of enterprise risk management: evidence from Canada. *Risk Management and Insurance Review*, 6, 53-73.

Kloman, F. (1992). Rethinking risk management. *The Geneva Papers on Risk and Insurance – Issues and Practice*, 17(3), 299-313.

Kloman, F. (2010). A brief history of risk management. In *Enterprise risk management: today's leading research and best Practices for tomorrow's Executives* (pp. 9-29). NJ: John Wiley & Sons.

Klugman, S.A., Panjee, H.H., & Willmot, G.E. (2004). *Loss models: from data to decisions*. NY: John Wiley & Sons.

Knight, F.H. (2006). *Risk, uncertainty and profit*. NY: Dover.

Knop, R., Ordovás, R., & Vidal, J. (2004). *Medición de riesgos de mercado y crédito*. Barcelona: Ariel Economía.

Kolluru, R.V. (1995). *Risk assessment and management: A unified approach. Risk assessment and management Handbook*. NY: McGraw-Hill.

Kozarevic, S., & Besic, N. (2015). Risk Management in telecommunications services in Bosnia and Herzegovina. *Ekonomski Vjesnik [Economic Journal]/ECONVIEWS*, 28, 9-24.

KPMG. (2020). *CEO Outlook 2020 Report. COVID-19 special edition*. Amstelveen: KPMG.

Krause, T.A., & Tse, Y. (2016). Risk management and firm value: recent theory and evidence. *International Journal of Accounting & Information Management*, 24(1), 56-81.

Kvale, S. (1996). *Interviews: an introduction to qualitative research interviewing*. London: Sage.

Lalonde, C., & Boiral, O. (2012). Managing risks through ISO 31000: a critical analysis. *Risk Management Journal*,14(4), 272-300.

Lechner, P., & Gatzert, N. (2018). Determinants and value of enterprise risk management: empirical evidence from Germany. *The European Journal of Finance*, 24.

Leitch, M. (2010). ISO 31000:2009 – the new international standard on risk management. *Risk Analysis Journal*, 30(6), 887-892.

Lewis, N. (2006). *Operational Risk*. London: John Wiley & Sons.

Liebenberg, A. P., Hoyt, R.E., & Kleffner, A.E. (2003). The determinants of enterprise risk management: evidence from the appointment of chief risk officers. Risk Management and Insurance Review, 6, 37-52.

Lundqvist, S. A. (2014). An explanatory study of enterprise risk management: pillars of ERM. *Journal of Accounting, Auditing and Finance*, 29(3), 393-429.

Lupton, D. (1999). *Risk*. London: Routledge.

Lynn, P., Turner, R., & Smith, P. (1998). Assessing the effects of an advance letter for a personal interview survey. *Journal of the Market Research Society*, 40(3), 265-272.

Manab, N.A., & Ghazali, Z. (2013). Does enterprise risk management create value? *Journal of Advanced Management Science* 1(4), 358-362.

Management Solutions. (2019). *Risk and internal control report. Challenges in the TMT industry*. Madrid: Management Solutions.

Martínez-Sánchez, J.F., Martínez-Palacios, M.T.V., & Venegas-Martínez, F. (2016). An analysis on operational risk in international banking: A Bayesian approach (2007-2011). *Estudios Gerenciales [Management Studies]*, 32, 208-220.

Matkin, G.W. (1990). *Technology transfer and the university*. NY: Macmillan.

McDonald, D., Bammer, G., & Deane, P. (2009). *Research integration using dialogue methods*. National Library of Australia: ANU E Press.

McShane, M.K. (2018). Enterprise risk management: history and a design science proposal. *Journal of Risk Finance*, 19(2), 137-153.

McShane, M.K., Nair, A., & Rustambekov, E. (2011). Does enterprise risk management increase firm value? *Journal of Accounting, Auditing and Finance*, 26(4), 641-658.

Meidell, A., & Kaarboe, K. (2017). How the enterprise risk management function influences decision-making in the organization – a field study of a large, global oil and gas company. *The British Accounting Review*, 49(1), 39-55.

Merton, R., & Peron, A. (1993). Theory of risk capital in financial firms. *Applied Corporate Finance*, 6(3), 16-32.

Mikes, A. (2009). Risk management and calculative cultures. *Management Accounting Research*, 20, 18-40.

Mikes, A., & Kaplan, R.S. (2013). *Managing risks: towards a contingency theory of enterprise risk management. Working Paper* (pp.13-63). Boston: Harvard Business School.

Moeller, R. R. (2007). *COSO enterprise risk management: understanding the new integrated ERM framework*. NJ: John Wiley & Sons.

Monda, B., & Giorgino, M. (2013). *An ERM maturity model*. ERM Symposium 2013 Monograph. Milan: Polytechnic University of Milan. NY/Amsterdam: Social Science Research Network/Elsevier.

Moosa, I., (2008). A critique of the advanced measurement approach to regulatory capital against operational risk. *Journal of Banking Regulation*, 9(3), 151-164.

Muermann, A., & Oktem, U. (2003). The near-miss management of operational risk. *The Journal of Risk Finance*, 4, 25-36.

Nieto Jiménez-Montesinos, M.A. (2005). *El tratamiento del riesgo operacional en Basilea II. Estabilidad Financiera*, 8. Madrid: Banco de España.

Nocco, B.W., & Stulz, R.M. (2006). Enterprise risk management: theory and practice. *Journal of Applied Corporate Finance*, 18(4), 8-20.

Orange Book. (2004). *Management of risk. Principles and Concepts*. HM Treasury. Norwich: HMSO.

Organization for Economic Cooperation and Development. (2014). *Risk management and Corporate Governance*. Corporate Governance. Paris: OECD.

Oxford Dictionary of English. (2010). *Oxford Dictionary of English*. OED: 3rd ed.

Pagach, D.P., & Warr, R. S. (2011). The characteristics of firms that hire chief risk officers. *The Journal of Risk and Insurance*,78(1), 185-211.

Pakhchanyan, S. (2016). Operational risk management in financial institutions: a literature review. *International Journal of Financial Studies*, 4, 20.

Panjer, H. (2006). *Operational risks: modelling analytics*. NY: John Wiley & Sons.

Payne, R.L., & Mansfield, R. (1973). Relationship of perceptions of organizational climate to organizational structure, context, and hierarchical position. *Administrative Science Quarterly*, 18(4), 515-526.

Patton, E., & Appelbaum, S.H. (2003). The case for case studies in management research. *Management Research News*, 26(5), 60-71.

Perera, A.S. (2019). Enterprise risk management-international standards and frameworks. *International Journal of Scientific and Research Publications*, 9(7), 211-217.

Pererva, P.G., Kocziszky, G., Szakály, D., & Somosi Veres, M. (2012). *Technology transfer* (monograph). Miskolc: University of Miskolc.

Perry, C. (2001). Case research in marketing. *The Marketing Review*, 1(3), 303-323.

Peters, J. (2020). *What is SOX compliance? Everything You Need to Know in 2019*. NY: Varonis Systems.

Pickett, K.H.S. (2005). *Auditing the risk management process*. NJ: John Wiley & Sons.

Proctor, T. (2014). *Creating problem solving for managers*. Oxfordshire: Routledge.

Project Management Body of Knowledge. (2008). *A guide to the Project Management Body of Knowledge (PMBOK)*. Pennsylvania: Project Management Institute (4th ed.).

Project Management Body of Knowledge. (2013). *A guide to the Project Management Body of Knowledge (PMBOK)*. Pennsylvania: Project Management Institute (5th ed.).

Project Management Body of Knowledge. (2020). *A guide to the Project Management Body of Knowledge (PMBOK)*. Pennsylvania: Project Management Institute (7th ed.).

Protiviti. (2006). *Guide to enterprise risk management. Frequently asked questions*. CA: Protiviti Independent Risk Consulting Publishing.

Purdy, G. (2010). ISO 31000:2009-setting a new standard for risk management. *Risk Analysis Journal*, 30(6), 881-886.

PwC. (2015). *PwC's Risk Radar. First to see. First to move*. London: PricewaterhouseCoopers.

PwC. (2021). *PwC's Risk Radar. Global Risks Horizon Draft Internal Report (working document)*. London: PricewaterhouseCoopers.

Quail, R. (2012). Defining your taste for risk. *Corporate Risk Canada*. Spring. 50-66.

Ramamoorti, S. (2003). *Internal auditing: history, evolution, and prospects*. The Institute of Internal Auditors Foundation. FL: IIA (The Institute of Internal Auditors).

Real Academia de la Lengua Española (RAE) [Spanish Language Royal Academy (RAE)]. (2014). *Diccionario de la lengua Española (DLE) [Spanish language dictionary (DLE)]*. RAE: 23rd ed.

Renn, O. (2008). Concepts of risk: an interdisciplinary review. *Journal of Ecological Perspectives for Science and Society* (GAIA), 17 (1), 50-66.

RepTrak. (2016). *2016 global RepTrak 100. The world's most reputable companies*. Boston: Reputation Institute Publishing.

Ringland, G. (2002). *Scenarios in business*. Chichester: John Wiley & Sons.

Risk and Insurance Management Society. (2009). *2008 financial crisis. A wake-up call for enterprise risk management*. NY: RIMS.

Risk and Insurance Management Society. (2011). *Why strategic management?* NY: RIMS.

Rubino, M. (2018). Comparison of the main ERM frameworks: how limitations and weaknesses can be overcome implementing IT governance. International *Journal of Business and Management*,13(12), 203.

Ruiz-Canela López, J. (2004). *La gestión por Calidad Total en la empresa moderna [Total quality management in the modern company]*. Madrid-CDMX: RA-MA.

Ruiz-Canela López, J. (2021). How Can Enterprise Risk Management Help in Evaluating the Operational Risks for a Telecommunications Company? *Journal of Risk and Financial Management*, 14(3), 139-165. MDPI AG.

Saleem, K.S.A., Zraqat, O.M., & Okuour, S.M. (2019). The effect of Internal Audit Quality (IAQ) on Enterprise Risk Management (ERM) in accordance to COSO framework. *European Journal of Scientific Research*, 152(2), 177-188.

Saunders, M., Lewis, P., & Thornhill, A. (2016). *Research Methods for Business Students*. London: Pearson Education.

Sehrawat, S. (2019). Risk management strategies in large telecom companies: with special reference to Nokia. *International Journal of Advanced Scientific Research and Management*, 4(2), 99-103.

Selim, G., & McNamee, D. (1999). Risk management and internal auditing: what are the essential building blocks for a successful paradigm change? *International Journal of Auditing*, 3(2), 147-155.

Siggelkow, N. (2007). Persuasion with case studies. *Academy of Management Journal*, 50(1), 20-24.

Silvestri, A., Arena, M., Cagno, E, Trucco, P., & Azzone, G. (2011). Enterprise risk management from theory to practice: the role of dynamic capabilities approach-the “Spring” Model”. In *Quantitative Financial Risk Management* (pp. 281-307). Heidelberg: Springer.

Simkins, B., & and Ramirez, S.A. (2008). Enterprise-wise risk management and corporate governance. *Loyola University Chicago Law Journal*, 39(3), 571-594.

Singh, N.P., & Hong, P.C.. (2020). Impact of strategic and operational risk management practices on firm performance: an empirical investigation. *European Management Journal*, 38, 723-735.

SOA. (2002). *Sarbanes-Oxley Act*. U.S. Securities and Exchange Commission (SEC). Washington: SOX/SOA.

Soriano, R. (2008). *Cómo se escribe una tesis. Guía práctica para estudiantes e investigadores*. Córdoba: Berenice.

Spira, L.F., & Page, M. (2003). Risk management: the reinvention of internal control and the changing role of internal audit. *Accounting, Auditing & Accountability Journal*, 16(4), 640-661.

Sriyalatha, M.A.K., & Fernando, K.P.P. (2015). *Risk Management practices on banks: evidence from Sri Lanka*. Proceedings of 12th International Conference on Business Management (ICBM). Sri Lanka: University of Sri Jayewardenepura.

Standards Australia/Standards New Zealand. (2004). *Risk management*. AS/NZS 4360. Sydney: AS/NZS.

Strzelczak, S. (2008). *Operational risk management*. Warsaw: Warsaw University of Technology Publication.

Swanepoel, E., Estehuysen, J., Vuuren, G., & Lotriet, R. (2017). Assessing reputational risk: a four point matrix. *Journal of Economic and Financial Sciences*, 10(2), 313-337.

Taleb, N. (2010). *The Black Swan. The impact of the highly improbable*. London: Penguin.

Tarantino, A. (2006). *Manager's guide to compliance. Best practices and case studies*. NJ: John Wiley & Sons.

Telco Group. (2020). *Annual Report*. Madrid: TELCO Group.

Thomas, J.L., & Pearson, N.D. (2000). Value at Risk. *Financial Analysts Journal* 2000, 56(2), 47-67.

Toneguzzo, J. (2010). How to allocate resources based on risk. In *Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives* (pp. 189–217). NJ: John Wiley & Sons.

Turnbull (1999). *Internal control: guidance for directors on the combined code*. The Committee on Internal Control (London Stock Exchange/Rank Group). London: The Turnbull Committee.

University of Georgia. (2005). Roundtable on enterprise risk management. *Journal of Applied Corporate Finance*, 8-25.

Urquijo, J.L. (1993). *Riesgos y decisiones*. Bilbao: Deusto.

Wade, K., & Wynne, A. (1999). *Control self-assessment for risk management and other practical applications*. NJ: John Wiley & Sons.

Wahlström, G. (2009). Risk management versus operational action: Basel II in a Swedish context. *Management Accounting Research*, 20(1), 53-68.

Wieczorek-Kosmala, M. (2014). Risk management practices from risk maturity models perspective. *Journal of East European Management Studies*, 19(2), 133-159.

Woods, M. (2009). A contingency theory perspective on the risk management control system within Birmingham City Council. *Management Accounting Research*, 20(1), 69-81.

Wu, T-C., Tsaur C-C., Lin, C-H., & Shiau, S-Y. (2011). Surveying Safety Culture in Telecommunications Industry. *Journal of Occupational Safety and Health*, 35, 403-420.

Yesuf, A.S. (2017). *A review of risk identification approaches in the telecommunication domain*. Proceedings of the 3rd International Conference on Information Systems, Security and Privacy (ICISSP). Porto: Goethe University of Frankfurt.

Yesuf, A.S. (2017). *A review of risk identification approaches in the telecommunication domain*. Porto: Third International Conference on Information Systems Security and Privacy (ICISSP) Paper (February) 19-21.

Yin, R. (1994). *Case study research: Design and methods*. CA: Sage.

6 APPENDICES

APPENDIX A

INTERVIEWERS´ GUIDE FOR RISK IDENTIFICATION AND EVALUATION

A. Overall risk perception and identification by levels 1 and 2 categories

Theoretical rationale: Analyze manager's "main issues" regarding operational risks associated with their business unit activities or about others where they have knowledge, interlocks or previous experience. This provides a basic reference framework to identify, classify and structure the different operational events in TELCO. The answers to these questions for every interviewee in the workshop allowed us to build the risk type groups (*) (event levels 1 and 2 categories). For example: Events Group 1 (level 1) category: End Customer and Sale of Products and Services. Level 2 category: 1.1 End customer; 1.2 Marketing and sale of products and services; 1.3 Customer service.

Question: Would you identify and describe the main issues associated with the risks you are familiar with (where "the shoe pinches")?

(*) Risk types groups (level 1): (1) end customer and sale of products and services; (2) poor quality/interruption of service; (3) failures/damage to assets (equipment, networks, systems, facilities, buildings); (4) suppliers, counterparties, contractors and other agents; (5) processes; (6) breach of/non-compliance with laws and standards; (7) fraud and unauthorized activities; (8) employment practices and on-the-job safety; and (9) harm to environment or to third parties.

B. Risk identification by level 3 category

Theoretical rationale: Once level 1 and level 2 categories of the identification framework have been structured, analyze manager's "main concepts" attached to the respective level 2 category in order to carry on with the identification and classification of the operational events with higher level of detail (level 3). This level 3, together with levels 1 and 2, define the operational risk identification frameworks, and therefore, the operational risk identification pillar for TELCO.

Questions: The basic question for every risk concept at level 2 is: "Is there any event or situation you consider a materialized or potential risk associated with…?"

Question 1.1: Is there any event or situation you consider a materialized or potential risk associated with end customer?

Question 1.2: Is there any event or situation you consider a materialized or potential risk associated with marketing and sale of products and services?

Question 1.3: Is there any event or situation you consider a materialized or potential risk associated with customer service?

Question 2.1: Is there any event or situation you consider a materialized or potential risk associated with poor quality / interruption of service?

Question 3.1: Is there any event or situation you consider a materialized or potential risk associated with failures / damages to equipment, network, systems, facilities and buildings?

Question 3.2: Is there any event or situation you consider a materialized or potential risk associated with non-availability to equipment, network, systems, facilities and buildings?

Question 3.3: Is there any event or situation you consider a materialized or potential risk associated with other outside events (e.g. third parties, animals, …) to equipment, network, systems, facilities and buildings?

Question 3.4: Is there any event or situation you consider a materialized or potential risk associated with accidents to equipment, network, systems, facilities and buildings?

Question 4.1: Is there any event or situation you consider a materialized or potential risk associated with non-availability at source of suppliers, counterparties, contractors and other agents?

Question 4.2: Is there any event or situation you consider a materialized or potential risk associated with delays and substandard quality in the services received from suppliers, counterparties, contractors and other agents?

Question 4.3: Is there any event or situation you consider a materialized or potential risk associated with conflicts and arbitration in agreements and contracts of suppliers, counterparties, contractors and other agents?

Question 5.1: Is there any event or situation you consider a materialized or potential risk associated with revenue assurance processes?

Question 5.2: Is there any event or situation you consider a materialized or potential risk associated with operation of equipment, network and systems?

Question 5.3: Is there any event or situation you consider a materialized or potential risk associated with formalization of contracts?

Question 5.4: Is there any event or situation you consider a materialized or potential risk associated with external and internal disclosure and reporting?

Question 5.5: Is there any event or situation you consider a materialized or potential risk associated with management of investments, stocks, other processes and transactions?

Question 6.1: Is there any event or situation you consider a materialized or potential risk associated with improper business practices?

Question 6.2: Is there any event or situation you consider a materialized or potential risk with intentional breach of internal policies?

Question 6.3: Is there any event or situation you consider a materialized or potential risk associated with other violations / non-compliance with laws, regulations and standards?

Question 7.1: Is there any event or situation you consider a materialized or potential risk associated with internal fraud or unauthorized activities?

Question 7.2: Is there any event or situation you consider a materialized or potential risk associated with external fraud?

Question 8.1: Is there any event or situation you consider a materialized or potential risk associated with occupational safety, health and hygiene?

Question 8.2: Is there any event or situation you consider a materialized or potential risk associated with relations, diversity and discrimination of employees?

Question 9.1: Is there any event or situation you consider a materialized or potential risk associated with environmental damage?

Question 9.2: Is there any event or situation you consider a materialized or potential risk associated with damage to third parties and to assets of third parties (excluding employees and customers)?

C. Risk evaluation

Theoretical rationale: Follow the operational risk self-assessment process and method in gathering the following information: (i) the risk thresholds (UL.I, UL.II, and UL.III) provided by the managers of the business unit (segments or organizational units); and (ii) inputs from the managers, i.e. the information of the three estimates of the analyzed event (frequency, severity, worst case) as well as the risk factor and comments on every event included in the respective question; and (iii) the outputs of the expected losses and unexpected losses, and the rating percentages (risk levels A, B, C and D) based on unexpected losses results. This process, as explained, was supported by the OpRISK SW. These results are the outcome of the operational risk evaluation pillar.

Questions: The basic question for every risk concept at level 3 is: “Is there any risk of losses associated with …?”. All the questions will be filled in by managers following the

OpRISK SW (see illustrative figures in the "execution of questionnaires" within the 3.2.2.1 sub-section (operational risk self-assessment process).

Table 6.1 provides an illustration (Fixed Line Business Unit – Residential Segment) of the various questions, including the event, frequency, severity and worst case (in €), its risk factor classification and comments, if filled in. In this case, the business unit reported the following risk thresholds: UL.I = 32,210,000 €; UL.II = 64,420,000 €; and UL.III = 96,630,000 €, as described in sub-section 3.3.1 (empirical results).

Table 6.1. Illustration of Executed Questionnaire of Residential Segment of Mobile Line Business Unit

Pregunta	**¿Existe el riesgo de sufrir perdidas asociadas a errores producidos durante el marketing y la comercialización de los productos o servicios?**
Evento	01_02 - Marketing y comercialización de Productos y Servicios
Frecuencia	Once in a year
Severidad	Between 16.000,00 and 50.000,00
Peor caso	For whichever value
Factor de riesgo	02_01 Suficiencia cualitativa
Comentarios	
Pregunta	**¿Existe el riesgo de sufrir perdidas asociadas a errores, fallos o mala calidad en la atención al cliente (pre-venta, post-venta y call centersl)?**
Evento	01_03 - Servicio a cliente
Frecuencia	Many times a day
Severidad	Between 27.000,00 and 61.000,00
Peor caso	Less than 750.000,00
Factor de riesgo	04_03 Contratas / outsourcing / terceros
Comentarios	Son 11.000 bajas al año con un ARPU de 420€.
Pregunta	**¿Existe el riesgo de sufrir perdidas asociadas a la mala calidad en la prestación del servicio de voz, datos, contenidos, etc. Debido a causas internas?**
Evento	02_01 - Mala calidad
Frecuencia	Many times a day
Severidad	Between 61.000,00 and 140.000,00
Peor caso	Less than 130.000,00
Factor de riesgo	04_03 Contratas / outsourcing / terceros
Comentarios	Son 44.000 bajas al año con un ARPU de 420€
Pregunta	**¿Existe el riesgo de sufrir perdidas asociadas a la mala calidad en la prestación del servicio de voz, datos, contenidos, etc. Como consecuencia de problemas con terceros (otros operadores, PAM Premium, proveedores, contratas…)?**
Evento	02_01 - Mala calidad
Frecuencia	Once in a day
Severidad	Between 34.000,00 and 79.000,00
Peor caso	Less than 1.100.000,00
Factor de riesgo	04_03 Contratas / outsourcing / terceros
Comentarios	

Source: OpRSA SW screen shot. Figures in €

Table 6.2 depicts an illustration (Mobile Line Business Unit – Residential Segment) of a summary report including the loss event type, the question and the results (expected loss and unexpected loss and rating).

Table 6.2. Results of Residential Segment of Mobile Line

	Loss Event Type		Question		Results		Rating			
	Code	Description			EL	UL	A	B	C	D
1	01_01	Cliente Final	1	¿Existe el riesgo de sufrir perdidas asociadas a reclamaciones relacionadas con la protección de datos al cliente?	€ 12.133	€ 158.407	100%	0%	0%	0%
2	01_01	Cliente Final	2	¿Existe el riesgo de sufrir perdidas asociadas a reclamaciones relacionadas con la prestación / provisión del servicio (averías, nivel de servicio, normativas de calidad...)?	€ 166.663	€ 112.065	100%	0%	0%	0%
3	01_01	Cliente Final	3	¿Existe el riesgo de sufrir perdidas asociadas a reclamaciones relacionadas con la medida / tarificación / facturación / cobro de productos o servicios?	€ 418.748	€ 281.562	100%	0%	0%	0%
4	01_01	Cliente Final	4	¿Existe el riesgo de sufrir perdidas asociadas a reclamaciones relacionadas con la atención al cliente (actual o potencial)?	€ 166.663	€ 112.065	100%	0%	0%	0%
5	01_02	Marketing y comercialización de productos y servicios	5	¿Existe el riesgo de sufrir perdidas asociadas a errores producidos durante el diseño (desarrollo comercial) de los productos o servicios?	€ 2.183.977	€ 8.130.400	1%	99%	0%	0%
6	01_02	Marketing y comercialización de productos y servicios	6	¿Existe el riesgo de sufrir perdidas asociadas a errores producidos durante el marketing y la comercialización de los productos o servicios?	€ 2.183.977	€ 8.130.400	1%	99%	0%	0%
7	01_03	Servicio a Cliente	80	¿Existe el riesgo de sufrir pérdidas asociadas a errores, fallos o mala calidad en la atención al cliente (pre-venta, post-venta, distribuidores y call centers)?	€ 772.567	€ 1.953.204	100%	0%	0%	0%
8	02_01	Mala calidad	8	¿Existe el riesgo de sufrir perdidas asociadas a la mala calidad en la prestación del servicio de voz, datos, contenidos, etc. Debido a causas internas?	€ 22.999.775	€ 22.940.289	0%	0%	4%	96%
9	02_01	Mala calidad	9	¿Existe el riesgo de sufrir perdidas asociadas a la mala calidad en la prestación del servicio de voz, datos, contenidos, etc. Como consecuencia de problemas con terceros (otros operadores, PAM Premium, proveedores, contratas...)?	€ 11.666.625	€ 13.209.924	0%	0%	100%	0%
10	02_01	Mala calidad	10	¿Existe el riesgo de sufrir perdidas asociadas a la mala calidad en la provisión del servicio a nuevos clientes?	€ 5.316.658	€ 6.233.223	0%	100%	0%	0%
11	04_01	Indisponibilidad en el origen	77	¿Existe el riesgo de sufrir perdidas asociada indisponibilidad en el origen de servicios, existencias, repuestos, equipos y sistemas?	€ 11.700.000	€ 8.951.367	8%	84%	8%	0%
12	04_02	Retrasos e incumplimiento de la calidad de los servicios recibidos	78	¿Existe el riesgo de sufrir perdidas asociada a retrasos e incumplimiento de la calidad de los servicios recibidos, existencias, repuestos, equipos y sistemas?	€ 1.645.488	€ 3.806.065	96%	4%	0%	0%
13	05_01	Proceso de aseguramiento de ingresos	22	¿Existe el riesgo de sufrir pérdidas asociadas a errores en el proceso de medición del tráfico, servicio, consumo, ...?	€ 630.702	€ 3.179.930	99%	1%	0%	0%
14	05_01	Proceso de aseguramiento de ingresos	23	¿Existe el riesgo de sufrir pérdidas asociadas a errores en el proceso de tarificación de los servicio contratados?	€ 245.051	€ 1.517.947	100%	0%	0%	0%
15	05_04	Comunicación y reporte interno	70	¿Existe el riesgo de sufrir pérdidas asociadas a errores y retrasos en la comunicación y reporte interno?	€ 57.790	€ 2.885.947	100%	0%	0%	0%
16	07_01	Fraude interno / actividades desautorizadas	33	¿Existe el riego de sufrir pérdidas asociadas al fraude interno y/o a actividades desautorizadas?	€ 3.467	€ 133.068	100%	0%	0%	0%
17	07_02	Fraude externo	34	¿Existe el riego de sufrir pérdidas asociadas al fraude externo?	€ 4.208.618	€ 2.794.795	100%	0%	0%	0%

Source: OpRSA SW screen shot. Figures in €

APPENDIX B

CERTIFICATE OF PUBLICATION OF THE ARTICLE "How can Enterprise Risk Management Help in Evaluating the Operational Risks for a Telecommunications Company"

Article publication requirement fulfilled (*el Art. 23.3. de la Normativa Reguladora de los Estudios de Doctorado de la Universidad Rey Juan Carlos establece que: "Para garantizar, con anterioridad a su presentación formal, la calidad del trabajo desarrollado, se aportará al menos una publicación aceptada o publicada en un medio de impacto en el ámbito de conocimiento de la tesis doctoral firmada por el doctorando, que incluya parte de los resultados de la tesis"*). Publication (23 March 2021): Ruiz-Canela López, J. (2021). "How Can Enterprise Risk Management Help in Evaluating the Operational Risks for a Telecommunications Company?" Journal of Risk and Financial Management (JRFM), 14(3), 139-165. MDPI AG. http://dx.doi.org/10.3390/jrfm14030139. This article and its certificate are submitted in addition to the doctoral thesis document. JRFM is an emerging JCR Journal indexed by the Web of Science Core Collection, ranked B in the Australian ABDC Journal Quality List, and indexed by Academic OneFile (Gale), DOAJ, EBSCO, EconBiz, EconLit, EconPapers/RePEc, ESCI / Web of Science, IDEAS /RePEc and ProQUest.


Journal of Risk and Financial Management

an Open Access Journal by MDPI

CERTIFICATE OF PUBLICATION

Certificate of publication for the article titled:

How Can Enterprise Risk Management Help in Evaluating the Operational Risks for a Telecommunications Company?

Authored by:

José Ruiz-Canela López

Published in:

J. Risk Financial Manag. **2021**, Volume 14, Issue 3, 139

MDPI Academic Open Access Publishing since 1996

Basel, March 2021

Universidad Rey Juan Carlos

RESUMEN DE LA TESIS DOCTORAL

CONSTRUCCIÓN DE UN MODELO DE GESTIÓN DE RIESGOS CORPORATIVOS (ERM) PARA LA IDENTIFICACIÓN Y EVALUACIÓN DE LOS RIESGOS OPERACIONALES DE UN EMPRESA DE TELECOMUNICACIONES. APLICACIÓN A UN CASO PRÁCTICO

Autor:

José Ruiz-Canela López

Director:

Dr. Francisco Javier Forcadell Martínez

Programa de Doctorado en Ciencias Sociales y Jurídicas

Línea de investigación: Empresa

Escuela Internacional de Doctorado

2021

1 RESUMEN GENERAL[1]

El riesgo operacional se define como las pérdidas potenciales resultantes de eventos causados por la inadecuación o fallos en los procesos, las personas, los equipos y sistemas o por factores externos. Uno de los retos más importantes para la gestión de la empresa es mejorar sus resultados mediante la identificación y evaluación del riesgo operacional. La mayor parte de los estudios sobre la gestión del riesgo empresarial (ERM) tiene su origen en el sector financiero y faltan estudios en otros sectores, como el de las telecomunicaciones. Este estudio de investigación propone un modelo innovador de identificación y evaluación de riesgos operacionales, basado en un enfoque de estudio del caso de una empresa de telecomunicaciones (TELCO), cuyos pilares principales son los modelos de identificación del riesgo operacional para los eventos, los factores de riesgo y los efectos del riesgo, así como el desarrollo de una metodología de evaluación del riesgo operacional, sobre la base de un proceso y un método de autoevaluación del riesgo operacional. El proceso de autoevaluación del riesgo operacional evalúa los riesgos operacionales a través de un análisis cuantitativo de estimaciones cuyas entradas son el impacto económico y la probabilidad de ocurrencia de los eventos. El método de autoevaluación del riesgo operacional es el "motor" para calcular el impacto económico del riesgo, aplicando técnicas actuariales, que permiten estimar las distribuciones de pérdidas inesperadas y esperadas en TELCO. Los resultados de las unidades de negocio analizadas en el trabajo de campo para el caso de estudio fueron comparados con calificaciones estandarizadas (aceptable, asumible, crítico o catastrófico), y contrastados con los gestores de la empresa, demostrando que el modelo de identificación y evaluación del riesgo operacional es una herramienta de gestión fiable y útil para la empresa y sus grupos de interés, y dando lugar a más investigaciones en otros sectores donde la gestión del riesgo operacional es clave para el éxito de la empresa.

El presente resumen de la tesis doctoral incluye los siguientes apartados, además del resumen general: (i) **antecedentes** (y conclusiones de la fundamentación teórica), (ii) **objetivos** (describiendo también las proposiciones de la investigación y su contribución científica), (iii) **metodología** (enfoque de estudio del caso, alcance de la investigación y técnicas de evaluación de riesgos y recopilación de datos), (iv) **resultados** empíricos y teóricos, así como (v) **conclusiones** (principales hallazgos, conclusiones del estudio

[1] Este documento no incluye citas ni referencias al tratarse de un “resumen de la tesis” en catellano elaborado por el autor (art. 22.2 de la “Normativa Reguladora de los Estudios de Doctorado”).

empírico, relación entre las proposiciones y los resultados obtenidos, y principales contribuciones e implicaciones prácticas.

2. ANTECEDENTES

Un aspecto común a cualquier decisión que tomemos, como individuos, grupos de personas u organizaciones, es que todos nos enfrentamos a la incertidumbre. El riesgo está en todas partes y se deriva directamente de la imprevisibilidad, tanto en las actividades de la vida cotidiana como en los procesos de toma de decisiones empresariales relevantes. La capacidad de prever lo que puede ocurrir en el futuro y de elegir entre alternativas es siempre un reto para las sociedades y empresas. Las consecuencias de los últimos acontecimientos en el mundo, como el terrorismo, la crisis financiera, las condiciones meteorológicas extremas o la actual pandemia mundial COVID-19, han hecho que el riesgo adquiera mayor relevancia. Estos riesgos extremos a los que se enfrentan las sociedades y las empresas coexisten con los riesgos mundanos antes mencionados. Sin embargo, las consecuencias de los acontecimientos a escala mundial y en la vida personal de las personas podrían incluir la creación de oportunidades nuevas y valiosas, como la apreciación de lo que tenemos como individuos y sociedad y de lo que queremos conservar para el futuro, en base a las lecciones aprendidas.

La definición de riesgo se refiere de algún modo a lo que la providencia depara, la contingencia o la proximidad del peligro; el concepto de riesgo suele entenderse como una posibilidad de peligro, pérdida, lesión u otras consecuencias adversas. En estas definiciones, el riesgo se utiliza para significar consecuencias negativas; sin embargo, asumir riesgos es la esencia de la gestión empresarial y de la vida cotidiana, ya que también pueden dar lugar a un resultado positivo (las oportunidades). Una definición básica es la combinación de la probabilidad de un evento y su consecuencia. Las consecuencias pueden ser tanto positivas como negativas. En este estudio se exploran otras definiciones de riesgo y de gestión de riesgos, creando un lenguaje común dentro de la organización, que es un factor clave de éxito para desplegar la gestión de riesgos.

Es relevante tener en cuenta que parte del enfoque moderno del riesgo proviene de una serie de grandes fracasos organizativos, gubernamentales y de escándalos financieros en las últimas décadas (Citigroup y Enron son sólo ejemplos de estas situaciones) que han centrado la atención de los reguladores, los inversores y los clientes en la forma en que los directivos están gestionando el riesgo. Asimismo, se recuerdan una serie de catástrofes operativas, como los atentados del World Trade Center del 11 de septiembre

de 2001 o el tsunami de Sumatra-Andamán del 26 de diciembre de 2004, como ejemplos de riesgos materializados.

Un aspecto común de las organizaciones es que se enfrentan a la incertidumbre en sus decisiones estratégicas y operativas, y la gestión de riesgos proporciona un marco para que las organizaciones se enfrenten a la incertidumbre. La práctica moderna de la gestión de riesgos es un enfoque sistemático, basado en normas exhaustivas que ayudan a mejorar la capacidad de recuperación de las empresas, aumentar la previsibilidad y cumplir el propósito fundamental de la organización empresarial mediante la creación de valor para las partes interesadas o grupos de interés. Éstas suelen estar representadas por los clientes, los accionistas, los empleados, los proveedores y por el impacto social que producen. Dos modelos principales -los marcos COSO-ERM (*Committee of Sponsoring Organizations of the Treadway Commission-Enterprise Risk Management*), y las normas ISO 31000 (*International Organization for Standardization*)- ayudan a gestionar los distintos tipos de riesgo a los que se enfrentan las organizaciones. La gestión del riesgo empresarial (ERM) facilita el conocimiento de los factores de riesgo, lo que ayuda a la dirección a tomar decisiones. Los marcos y normas COSO-ERM e ISO 31000 se centran en el despliegue de un proceso teórico de gestión de riesgos para la empresa. En concreto, ERM se puede entender como un proceso efectuado por el consejo de administración de una entidad, su dirección y el personal, aplicable a la definición de estrategias en toda la empresa y diseñado para identificar eventos potenciales que puedan afectar a la organización, gestionar sus riesgos del riesgo aceptado y proporcionar una seguridad razonable sobre el logro de los objetivos.

Tal como se discute en la fundamentación teórica de la investigación, la identificación y la evaluación de riesgos son los pasos más importantes del proceso de gestión de riesgos con el objetivo de mejorar los resultados de la empresa, siendo los riesgos operacionales los eventos más básicos y comunes para cualquier unidad de negocio de una organización. Sin embargo, la normativa publicada en materia de riesgos tiene algunas limitaciones, como la falta de técnicas de identificación y evaluación de riesgos para ser desplegadas en sectores específicos (por ejemplo, las telecomunicaciones).

En resumen, siendo uno de los retos más importantes para la gestión de la empresa mejorar sus resultados a través de su identificación y evaluación del riesgo operacional, el objetivo central de esta investigación es la creación y aplicación de un modelo innovador para ayudar a los directivos de las empresas, investigadores y profesionales

en la obtención de conocimientos y la aplicación práctica de la disciplina de gestión de riesgos dentro del sector de las telecomunicaciones. La contribución científica desarrollada en esta investigación, conocida como transferencia de conocimientos o transferencia tecnológica, pretende ayudar a las organizaciones a alcanzar el reto mencionado de mejorar sus resultados operativos y financieros.

La tesis se organiza de la siguiente manera. Después de incluir una introducción, los objetivos de la investigación (propósito principal y preguntas de investigación) y la contribución científica, en la fundamentación teórica presentamos y explicamos los fundamentos de la gestión de riesgos, una revisión bibliográfica sobre estudios anteriores sobre la identificación y evaluación de los riesgos operacionales, el contexto actual de los riesgos en el sector de las telecomunicaciones, algunas conclusiones teóricas y las proposiciones de la investigación. A continuación, presentamos el estudio empírico, que incluye el diseño de la investigación y el desarrollo de los objetivos de la misma, es decir, el modelo y los resultados, en la identificación y evaluación de los riesgos operacionales para una empresa de telecomunicaciones. Por último, en las conclusiones, incluimos los principales hallazgos, las contribuciones e implicaciones prácticas para investigadores y profesionales, las futuras líneas de investigación, las limitaciones y las implicaciones para la gestión.

Conclusiones de la fundamentación teórica

La fundamentación teórica se ha estructurado en tres áreas básicas: fundamentos de la gestión de riesgos, estudios previos sobre la identificación y evaluación de los riesgos operacionales, así como revisión de los riesgos de negocio y operacionales en el sector de las telecomunicaciones (2020). A partir de ahí y de los objetivos de la investigación (propósito principal y preguntas de investigación), derivamos las proposiciones de la investigación.

En cuanto a los fundamentos de la gestión de riesgos, se ha realizado una revisión de la evolución de la disciplina de gestión de riesgos, analizando su impacto y sus definiciones básicas asociadas al concepto de riesgo y de gestión de riesgos, destacando el concepto de riesgo como oportunidad de negocio y la necesidad de crear un lenguaje común para acometer las proposiciones centrales de la investigación. Esta base común es necesaria porque la interrelación con los directivos es esencial para desarrollar el estudio de caso de TELCO, la empresa de telecomunicaciones elegida.

Además, se revisaron los principales marcos de gestión de riesgos, normas y comisiones asociadas. Este análisis ha permitido corroborar la generalidad de estos modelos teóricos, al tiempo que se ha puesto de manifiesto la importancia otorgada a las etapas de identificación y evaluación de riesgos, COSO II, junto con algunas técnicas derivadas de la norma ISO 31000. Estos constituyen un buen punto de partida teórico para el desarrollo de la investigación empírica.

A continuación, se realizó una revisión bibliográfica con la idea de encontrar un modelo sólido en el que basar la investigación; en este sentido, se puso de manifiesto la falta de estudios aplicables a las empresas del sector de las telecomunicaciones para la identificación y evaluación de sus riesgos operacionales. Sin embargo, fue posible explorar los avances de las empresas financieras, con gran experiencia y conocimiento en estas materias, que inspiraron la formulación del modelo de investigación propuesto mediante la extrapolación de ciertas técnicas cuantitativas y cualitativas. En concreto, Basilea II ha sido una fuente de inspiración para desarrollar el modelo, teniendo en cuenta que su aplicación se centra únicamente en el sector bancario.

Por último, a pesar de estar fuera del ámbito temporal de esta investigación, se han revisado los principales riesgos actuales, a fecha de los informes recientemente publicados y referidos al año 2020. Esta revisión da un sentido de actualidad a la investigación, incluyendo el actual riesgo global de la crisis pandémica. También proporciona información sobre los principales riesgos de las cuatro grandes empresas auditoras (Big Four) que tienen permanentemente radares para su detección, identificación y evaluación.

En resumen, las **conclusiones más importantes derivadas de la fundamentación teórica** son las siguientes:

- Se cumple la característica de transferencia tecnológica descrita en la contribución científica, es decir, la transferencia de conocimientos en la disciplina de la gestión de riesgos (investigadores, profesionales, gestores, académicos, entre otros).
- Se identifica la importancia y el tratamiento que otros estudios, modelos y normas dan a las etapas de identificación y evaluación de riesgos.
- Se ha identificado que las normas, marcos y modelos revisados no cumplen con los objetivos de esta investigación, de ahí la necesidad de este estudio. Esto es especialmente relevante en el caso de una empresa de telecomunicaciones, donde la revisión teórica y bibliográfica revela lo siguiente: (i) existencia de

modelos robustos de evaluación del riesgo operacional en el sector financiero; (ii) falta de estudios de modelos de gestión del riesgo operacional en el sector de las telecomunicaciones; y (iii) complejidad de las normas y marcos a implantar en una empresa con un enfoque comprensible y práctico (no tan teórico).

- Para formular un modelo de identificación y evaluación de riesgos se requiere un proceso ágil, útil y aplicable. Los procesos de gestión de riesgos revisados tanto en las normas ISO como en los marcos COSO proporcionan procesos demasiado teóricos y complejos para ser aplicados a una empresa como TELCO, o a cualquier otra empresa de su sector o incluso de otra industria donde haya empresas grandes y complejas. Por lo tanto, se ha desarrollado un marco para un proceso de gestión de riesgos basado en los fundamentos de la gestión de riesgos y en la revisión de la literatura.
- Finalmente, a partir de la revisión de los fundamentos teóricos, se incluyeron las proposiciones de investigación alineadas con el propósito principal y las preguntas de investigación de este estudio, basadas en los objetivos de la investigación y las conclusiones teóricas.

3. OBJETIVOS

Existen oportunidades para generar modelos de gestión de riesgos para la creación de valor en las empresas de telecomunicaciones, a pesar de que: (i) varios estudios de gestión de riesgos empresariales cuestionan la validez de estos modelos argumentando que pueden resultar enfoques teóricos y demasiado generales para tener una aplicación práctica exitosa en las empresas; y (ii) esta limitación es mayor respecto al reto de identificar y evaluar los riesgos operacionales para una gran empresa de telecomunicaciones, donde se carece de estudios contrastados frente a todos los modelos de valoración (identificación y evaluación) implantados en el sector financiero. Así, el **objetivo principal** de este estudio es crear y aplicar un modelo de identificación y evaluación de riesgos operacionales para una empresa del sector de las telecomunicaciones.

A partir de este propósito principal, las **preguntas de investigación** asociadas son:

- Pregunta de investigación I: ¿Cómo puede una empresa de telecomunicaciones identificar sus riesgos operacionales?
- Pregunta de investigación II: ¿Cómo puede una empresa de telecomunicaciones evaluar sus riesgos operacionales?

En resumen, las proposiciones de esta investigación fueron formuladas, a partir del propósito principal del estudio y de las preguntas de investigación, y una vez desarrollada la base teórica que sustenta el estudio empírico. Se refieren a la creación y aplicación de un modelo de identificación y evaluación de los riesgos operacionales para una empresa del sector de las telecomunicaciones a partir de: (i) las conclusiones teóricas; y (ii) la formulación de un marco de proceso de gestión de riesgos ágil, útil y práctico (fácil de aplicar) que contiene dos pasos básicos: la identificación y la evaluación de riesgos.

Proposiciones de la investigación

Una vez estudiados los contenidos básicos de la fundamentación teórica y considerando el propósito principal, las preguntas de investigación y los objetivos formulados en esta investigación, se procede a incluir dos proposiciones específicas. Estas proposiciones fueron analizadas en el estudio empírico y los resultados muestran hasta qué punto la evidencia del estudio de caso y los modelos creados las apoyan. Ambas proposiciones se basan en las dos etapas (identificación y evaluación) del proceso de gestión de riesgos descrito.

A partir del propósito principal, que es la posibilidad de crear y aplicar un modelo de identificación y evaluación del riesgo operacional para una empresa del sector de las telecomunicaciones, **las proposiciones específicas de la investigación** son las siguientes:

1. Es posible crear modelos de identificación de los riesgos operacionales de una empresa de telecomunicaciones para una gran empresa de este sector.
2. Es posible desarrollar una metodología de valoración y aplicarla para evaluar los riesgos operacionales de una empresa de telecomunicaciones para una gran empresa de este sector.

Contribución científica

La gestión del riesgo empresarial tiene sus raíces en la disciplina de las finanzas/ gestión del riesgo y los seguros (RMI). De hecho, las experiencias más estudiadas y probadas sobre el uso de métodos de identificación y evaluación del riesgo operacional pertenecen a las disciplinas financiera y de seguros, principalmente en el sector bancario, a través de modelos como el de Basilea II. En el sector de las

telecomunicaciones, hay escasa investigación en la creación de modelos de gestión de riesgos.

Además, aunque diversos trabajos científicos muestran que existe un consenso generalizado en que el crecimiento de la popularidad de los modelos COSO-ERM y de las normas ISO 31000 ha sido el resultado de una respuesta a la presión ejercida sobre las organizaciones para que gestionen el riesgo de forma holística, sin embargo, otros estudios cuestionan la validez de estos modelos y normas argumentando que pueden resultar demasiado teóricos y generales para tener una implantación práctica exitosa en las empresas. Incluso con el prominente modelo COSO-ERM y la norma de gestión de riesgos ISO 31000, aceptada en todo el mundo, los contextos organizativos hacen inviable un proceso de aplicación de la ERM a medida, especialmente en el sector de las telecomunicaciones debido a la falta de investigación mencionada.

Este estudio de investigación aborda las limitaciones anteriores. Su **objetivo** es crear, describir y aplicar un **modelo de identificación y evaluación de los riesgos operacionales** para una empresa del sector de las telecomunicaciones. Basado en un enfoque de estudio del caso, los principales pilares del modelo para las empresas del sector de las telecomunicaciones son: (i) los **modelos de identificación** de eventos, factores de riesgo y efectos del riesgo (OpRIF-*Operational Risk Identification Frameworks*); y (ii) el desarrollo de una **metodología de evaluación** de riesgos (OpRAM-*Operational Risk Assessment Model)*, apoyada en un **proceso y método de autoevaluación** del riesgo operacional (OpRSA-*Operational Risk Self-Assessment*). El proceso OpRSA evalúa los riesgos operacionales a través de un análisis cuantitativo de estimaciones, cuyos *inputs* son el impacto económico y la probabilidad de ocurrencia de eventos. El método OpRSA es el "motor" para calcular el impacto del riesgo económico, aplicando técnicas actuariales que estiman las distribuciones de pérdidas inesperadas y pérdidas esperadas en TELCO. Los resultados de las unidades de negocio analizadas se compararon con calificaciones estandarizadas (aceptable, asumible, crítico o catastrófico), y se contrastaron con los gestores de la empresa. Esto demostró que el marco OpRSA es una herramienta de gestión fiable y útil para la empresa, y da lugar a más investigaciones en otros sectores en los que la gestión del riesgo operacional es clave para el éxito de la empresa. Las empresas que implantan modelos de gestión de riesgos basados en ERM para la identificación y evaluación de riesgos obtienen altos resultados financieros y reciben las mejores evaluaciones del mercado.

Además, la contribución científica de este estudio se prevé teniendo en cuenta los objetivos de investigación mencionados y cuatro características destinadas a alcanzarlos: (i) **transferencia tecnológica**; (ii) **relevancia**; (iii) **originalidad**; y (iv) **no trivialidad.** En cuanto a los objetivos de la investigación, la contribución científica tendrá éxito si el modelo de identificación y evaluación del riesgo operacional creado es sólido, útil y práctico. Un breve resumen de los **objetivos de la contribución científica** incluye lo siguiente: (i) creación de un modelo innovador de riesgo operacional basado en modelos ERM universalmente aceptados, donde existe una falta de literatura y experiencias para el sector de las telecomunicaciones; (ii) aplicación real del modelo a una empresa compleja de telecomunicaciones, donde los modelos, procesos y métodos pueden ser extrapolados a otras empresas e industrias de diferentes sectores, para mejorar sus resultados de negocio, y por lo tanto, la satisfacción de las partes interesadas; (iii) el desarrollo de contribuciones clave para la gestión en términos de identificación y evaluación del riesgo operacional, estableciendo una "herramienta" empresarial como mejor práctica para ayudar a los directivos de las empresas en sus procesos de toma de decisiones; y (iv) el despliegue de implicaciones prácticas para la gestión de la empresa y para los investigadores y profesionales, contribuyendo al entorno empresarial y a la comunidad académica en la consolidación de conceptos teóricos y un enfoque práctico para la disciplina de ERM.

4. METODOLOGÍA

El estudio empírico de esta investigación se basa en las aportaciones teóricas estudiadas, y debe contribuir al cumplimiento de los objetivos de la investigación. La fundamentación teórica, a pesar de mostrar que apenas existe literatura para el desarrollo de la investigación en el sector de las telecomunicaciones, ha permitido identificar técnicas de identificación y evaluación de riesgos aplicadas en instituciones financieras que pueden ser extrapoladas a otros sectores (particularmente en la medición del riesgo basada en distribuciones de pérdidas). En este sentido, los estudios previos sobre la identificación y evaluación del riesgo operacional han permitido descartar ciertos enfoques que no son aplicables a sectores no financieros, pero también han aportado conceptos y líneas de trabajo que se utilizan en este estudio empírico. Además, conceptos analizados en esta literatura, como la autoevaluación, aportan información y conocimiento para el desarrollo del modelo de identificación y evaluación del riesgo operacional objeto de estudio. La norma ISO/IEC 31010 constituye una importante contribución a las técnicas de evaluación utilizadas. Asimismo, la revisión de los procesos de gestión de riesgos basada en las normas ISO 31000 y el

modelo COSO ha permitido conocerlos y simplificarlos. Además, un marco de procesos de gestión de riesgos eficaz es básico para que el estudio empírico describa las etapas de identificación y evaluación de riesgos, y su aplicación a TELCO. Por último, crear un lenguaje común y una cierta "cultura del conocimiento" sobre los riesgos a través de la revisión de los fundamentos de la gestión de riesgos es clave para el desarrollo del estudio empírico.

Para entender la metodología de esta investigación, se consideraron los siguientes contenidos: (i) enfoque de estudio del caso; (ii) alcance de la investigación; y (iii) técnicas de evaluación de riesgos y recopilación de datos.

Enfoque de estudio del caso

El objetivo principal de este estudio, tal como se enuncia en la sección de resultados, se centra precisamente en crear, describir y aplicar un modelo de identificación y evaluación de riesgos operacionales basado en los dos pilares mencionados, también objeto de construcción: los modelos de identificación del riesgo operacional (OpRIF) y la metodología de evaluación del riesgo operacional (RAM) que integra. La RAM integra dos componentes interrelacionados: un proceso de autoevaluación del riesgo operacional (proceso OpRSA) y un método de autoevaluación del riesgo operacional (método OpRSA). Ambos pilares se han construido, ilustrado y analizado mediante un enfoque de estudio de caso, aplicado a una empresa de telecomunicaciones global específica (TELCO) del Grupo TELCO. El estudio del caso de la empresa TELCO, tal y como se describe en el análisis de resultados, está alineado con el propósito principal descrito en los objetivos de la investigación de crear y aplicar un modelo de identificación y evaluación de los riesgos operacionales para una empresa del sector de las telecomunicaciones. El estudio aporta razones para legitimar el uso de la metodología de estudio del caso para una empresa como TELCO.

Alcance de la investigación

Se analizó la metodología para definir el alcance de los pilares de identificación y evaluación de riesgos en TELCO. Pueden seguirse dos enfoques diferentes en función del nivel de detalle deseado dentro de la estructura organizativa de TELCO:

- *Bottom-up vs. Top-down* (diferentes niveles de investigación en función de la información requerida y del nivel de detalle de las preguntas y respuestas en el proceso de recogida de datos).

- Totalidad vs. Parcialidad (diferentes ámbitos de aplicación, es decir, toda la empresa vs. unidades específicas y relevantes de la empresa).

Tanto para el pilar de identificación de riesgos como para el de evaluación de riesgos, el ámbito que decidimos que para TELCO fuera el enfoque *Top-down* y parcial (las razones se incluyen en el estudio). Tomamos esta decisión basándonos en el compromiso de los directivos en su papel de entrevistados, el número de unidades de negocio y de apoyo implicadas para la identificación de los eventos de TELCO y las unidades de negocio (Línea Fija y Línea Móvil) para aplicar la metodología de evaluación de riesgos.

Técnicas de evaluación de riesgos y recopilación de datos

Las referencias fundamentales para la definición de los aspectos metodológicos de este estudio están incluidas en las normas internacionales ISO 31010 e ISO/IEC 31010, que desarrollan y sugieren las principales técnicas de identificación y evaluación de riesgos. Asimismo, el desarrollo de la metodología de evaluación del riesgo operacional se basó en el uso de análisis de recolección de datos, a través de cuestionarios respondidos por los gerentes de TELCO, técnicas estadísticas sobre distribuciones de pérdidas operacionales, herramientas de evaluación de riesgos, así como la aplicación de enfoques de autoevaluación de control y riesgo, análisis actuarial, técnicas de evaluación probabilística de riesgos, recomendaciones de Basilea II, así como los modelos COSO y la normativa ISO 31000.

Para el pilar de identificación de riesgos, participaron directivos de las unidades de negocio de TELCO. A partir de la identificación de los eventos operativos de TELCO, los factores de riesgo y los efectos del riesgo, utilizamos datos primarios (temas tratados en talleres y entrevistas), apoyados por cuestionarios y datos secundarios (información interna clave de TELCO que poseen y utilizan los directivos). Realizamos talleres con las principales unidades de negocio de TELCO y entrevistas en profundidad con los directivos de las unidades de apoyo de TELCO. En ambos casos, las sesiones de brainstorming con preguntas semiestructuradas fueron herramientas útiles.

Para el pilar de evaluación de riesgos, se contó con la participación de directivos de las unidades de negocio de Línea Fija y Línea Móvil, que son las que están bajo el alcance de esta investigación para su evaluación, concretamente, los segmentos o unidades organizativas analizadas en la unidad de negocio de Línea Fija y los segmentos o áreas

organizativas incluidas en la unidad de negocio de Línea Móvil. Entrevistando a los directivos con conocimientos que eran responsables de los riesgos operacionales en las dos unidades de negocio relevantes en el ámbito del estudio, cumplimos los requisitos de muestreo intencionado de competencia y experiencia. Realizamos cuestionarios, uno por cada segmento o unidad organizativa, con el apoyo de talleres semiestructurados, siguiendo las directrices de la norma ISO 31010, lo que nos permitió mejorar los cuestionarios mediante la incorporación de datos secundarios adicionales en el diseño de la lista de control de las entrevistas, basándose en las ideas sugeridas por los directivos entrevistados como informantes clave, y posibilitando la presentación de contenidos enriquecidos a medida que los seguimientos con los directivos aclaraban cuestiones que se habían discutido en entrevistas anteriores. También realizamos entrevistas en profundidad con los directivos de ambas unidades de negocio principales. La información obtenida y apoyada por el software de la empresa, OpRisk, arrojó luz sobre los requisitos de entrada (frecuencia media estimada, severidad media estimada e impacto medio del peor caso estimado) convirtiéndola en los resultados (distribuciones de pérdidas y clases de riesgo). Además, para la metodología de evaluación del riesgo operacional, sobre la base de un proceso y método de autoevaluación del riesgo operacional, se ha utilizado el enfoque de autoevaluación del riesgo de control (CSA). La CSA es una potente herramienta de apoyo a los marcos de gestión de riesgos, y consiste en conseguir que los directivos y el equipo de trabajo autoevalúen la información sobre el riesgo, normalmente en talleres y reuniones facilitadas, como es el caso de TELCO.

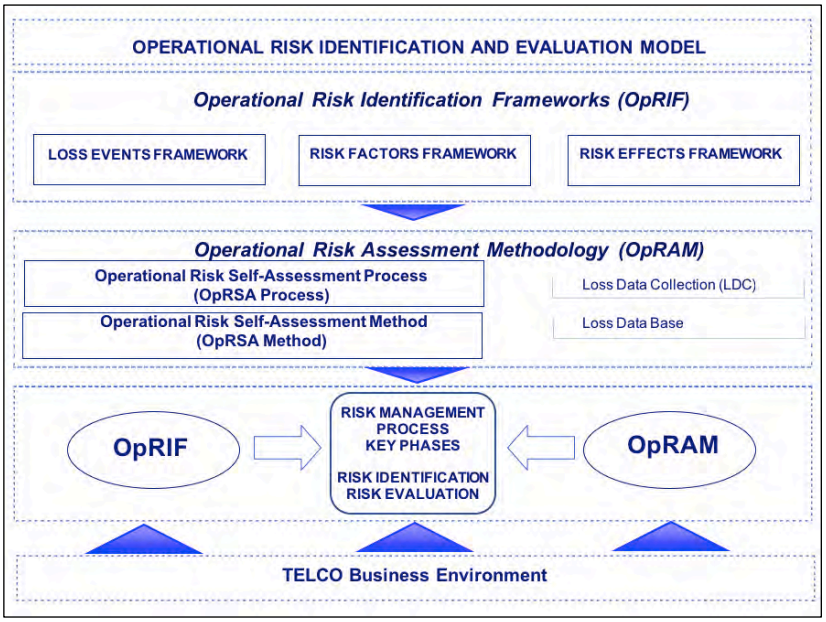
5. RESULTADOS

Como se ha mencionado, tras la definición del riesgo operacional para TELCO, el objetivo principal de este estudio ha sido la creación de un **modelo de identificación y evaluación de riesgos operacionales**, tal como se muestra en la siguiente **figura A** (original extraída de la tesis como figura 3.3), considerando los componentes del marco COSO y la norma ISO 31000.

- El primer pilar del modelo, la identificación del riesgo operacional, permitió establecer una **tipología en grupos de riesgos** para clasificar e identificar todos los fallos operacionales o posibles eventos de pérdida. Se trata de los modelos de definición e identificación del riesgo operacional (OpRIF),

- El segundo pilar del modelo que creamos es la **metodología de evaluación del riesgo operacional** (OpRAM), cuyos dos componentes son el **proceso y el método de autoevaluación del riesgo** (OpRSA). Para cada unidad organizativa en el ámbito del estudio de caso de TELCO, se realizó **un análisis cuantitativo de las estimaciones subjetivas** cuyos *inputs* son el impacto económico y la probabilidad de ocurrencia de cada evento para calcular las pérdidas esperadas, inesperadas y las clases de calificación para la evaluación de riesgos, aplicando técnicas actuariales.

Fig. A. Modelo de identificación y evaluación de riesgos operacionales. Fuente: elaboración propia



Resultados empíricos

El estudio muestra los resultados empíricos aplicados al estudio del caso TELCO sobre la base de los modelos de identificación del riesgo operacional y la aplicación de la metodología de evaluación del riesgo operacional, cuyos principales componentes son: las entradas de los cuestionarios (frecuencia media, severidad media y peor caso), la evaluación económica de los resultados en términos de pérdida esperada (EL) y pérdida inesperada (UL), el Valor en Riesgo (definido como la suma de EL y UL que expresa la pérdida máxima esperada en un año con un nivel de confianza del 99.9%), y los tres umbrales de riesgo que identifican las cuatro clases de calificación (aceptable, asumible, crítico, catastrófico). Todo ello expresado en forma de tablas en el estudio, así como la interpretación de esta información.

Resultados teóricos

Para dar una interpretación adecuada a esta investigación, es importante resumir algunas **cuestiones clave reveladas por la revisión bibliográfica** para conectar los resultados de este trabajo con estudios anteriores: (i) muchas empresas pertenecientes a diversos sectores siguen con el reto de implantar técnicas de identificación y evaluación de riesgos basadas en un enfoque de ERM; (ii) en general, el ERM ha atraído poca atención de la investigación en comparación con otras disciplinas; (iii) el enfoque de gestión de riesgos se encuentra en un estado de madurez para las empresas financieras, en particular en lo que respecta a las técnicas, métodos y herramientas avanzadas para la evaluación del riesgo operativo; (iv) la evaluación del riesgo operacional para las empresas no financieras no es una práctica fácil; (v) hay una falta de investigación en ERM para las empresas no financieras, en particular para las del sector de las telecomunicaciones; (vi) el ERM y sus metodologías asociadas deben implantarse en cualquier tipo de organización, independientemente de su sector, para crear valor para sus partes interesadas; (vii) no se ha encontrado y aplicado en el sector de las telecomunicaciones ninguna metodología práctica de evaluación de riesgos basada en la autoevaluación de riesgos y en el análisis de escenarios con el enfoque estadístico y actuarial utilizado en las empresas financieras; y (viii) la investigación basada en estudios de casos ha demostrado ser una buena práctica en los estudios de ERM para construir, contrastar e ilustrar los resultados de la implantación del ERM.

Los resultados muestran que es posible y útil construir marcos prácticos de identificación de riesgos y una metodología de evaluación (proceso y método) para ayudar a una empresa de telecomunicaciones (TELCO) a evaluar sus riesgos operacionales. De hecho, los resultados de esta investigación conducen a un enfoque práctico de identificación y evaluación de riesgos para el negocio de una gran empresa, en contraste con otros estudios teóricos que se centran en los fundamentos del proceso de ERM.

Otro resultado de este estudio es la convergencia entre las prácticas teóricas y las ilustradas por el estudio de caso de TELCO en la construcción de una herramienta de gestión práctica para apoyar los procesos de toma de decisiones en una empresa. Esto se describe, una vez identificados los riesgos, en las fases del proceso OpRSA y su método OpRSA incorporado. En este sentido, **dos aspectos innovadores** resultantes de este estudio son: (i) la utilización, mejora y aplicación del marco conceptual COSO ERM para la identificación y evaluación de los riesgos operacionales; y (ii) la extrapolación y adaptación de métodos y técnicas de uso común en el sector financiero a TELCO. Estos dos aspectos deben situarse en el contexto de que, aunque los

académicos están examinando cada vez más la adopción y el impacto del ERM, sus estudios suelen ser demasiado generales y poco concluyentes debido a una especificación inadecuada de cómo se utiliza el ERM en la práctica, aplicando una metodología específica para su aplicación. Esta idea se extiende a la creación y aplicación de la metodología de evaluación de riesgos y se debe al desconocimiento de las técnicas de gestión de riesgos específicas para grandes sectores no financieros como el de las telecomunicaciones. Para una gran organización como TELCO, ha sido práctico organizar talleres y cuestionarios regulares para la recopilación de datos y la técnica de autoevaluación de riesgos para el trabajo de campo de las unidades de negocio elegidas, junto con los representantes clave del negocio (directivos). Este enfoque fue dirigido y apoyado por la alta dirección para garantizar que el proceso de OpRSA se llevara a cabo con rigor.

6. CONCLUSIONES

Principales hallazgos

Existe un consenso generalizado de que el crecimiento de la popularidad de los marcos de gestión de riesgos empresariales (ERM) ha sido el resultado de una respuesta a las exigencias de las organizaciones para gestionar el riesgo. Sin embargo, varios estudios de ERM cuestionan la validez de estos modelos, argumentando que al ser aceptados en las comunidades que estudian la gestión de riesgos, pueden resultar modelos teóricos y generales para tener una aplicación práctica exitosa en las empresas. Esta limitación es aún mayor respecto al reto de identificar y evaluar los riesgos operacionales para una gran empresa de telecomunicaciones, donde se carece de referencias contrastadas frente a todos los modelos de evaluación implantados en el sector bancario. Este estudio ha intentado examinar cómo las empresas de telecomunicaciones pueden identificar y evaluar sus riesgos operacionales a partir de un caso práctico. El modelo de identificación y evaluación del riesgo operacional presenta los modelos, el proceso y el método pertinentes, incluidos los pasos que los profesionales pueden encontrar útiles y significativos para las empresas de telecomunicaciones. Además, el modelo propuesto y sus resultados, principal contribución de esta investigación, fueron validados empíricamente con directivos de TELCO y mostraron altos niveles de fiabilidad y validez. Este estudio pone de manifiesto que, en un mundo empresarial dinámico y complejo, los modelos ERM pueden adaptarse a las necesidades de las empresas, en particular para gestionar sus riesgos operacionales con el fin de mejorar el rendimiento y la creación de valor. Incluso con dos destacados marcos de ERM (COSO ERM e ISO 31000), los contextos organizativos

hacen imposible un método único de aplicación de la ERM, y ésta es la razón fundamental para investigar la creación de modelos innovadores de identificación de riesgos operacionales (OpRIF) y metodologías de evaluación similares, como la OpRAM (metodología de evaluación de riesgos operacionales).

En resumen, las **principales conclusiones de esta investigación sobre la transferencia tecnológica** (transferencia de conocimiento) son las siguientes:

- Los estudios de ERM de algunas organizaciones revelan su impacto limitado en los resultados de sus operaciones, ya que se consideran demasiado genéricos y teóricos. De hecho, sobre la base de la literatura revisada, no existen actualmente referencias prácticas y probadas sobre la aplicación de modelos de gestión para la identificación y valoración (evaluación) de los riesgos operacionales en el sector de las telecomunicaciones;
- La creación de un proceso de gestión de riesgos simplificado y de fácil comprensión, basado en las normas y marcos más reconocidos en la disciplina de riesgos, para la selección de las dos fases más importantes de este proceso y su categoría de riesgo: la identificación y la evaluación de los riesgos operacionales;
- La identificación de los eventos operacionales, los factores de riesgo y los efectos basados en el estudio del caso TELCO;
- El desarrollo de una metodología de evaluación de los riesgos operacionales, basada en el estudio del caso TELCO, a partir de un proceso y un método de autoevaluación de los riesgos;
- Como parte del diseño de la investigación, la metodología y las técnicas utilizadas para el estudio empírico, así como la empresa de telecomunicaciones seleccionada como caso de negocio, han arrojado resultados empíricos y conceptuales que corroboran, confirman, validan y apoyan la propuesta principal y los objetivos de este estudio.
- Es definitivamente factible, relevante, práctico y útil para diferentes grupos (por ejemplo, directores, ejecutivos, investigadores, profesionales, y la academia y las organizaciones, en general) identificar un modelo de identificación y evaluación del riesgo operacional aplicado al sector de las telecomunicaciones, a partir de su aplicación a un caso de empresa (TELCO) y extrapolado a otras empresas del mismo sector, e incluso a otro tipo de industrias; y finalmente,
- Las conclusiones de este estudio de investigación revelan las aportaciones, las implicaciones prácticas, las investigaciones futuras y las limitaciones, así como

las lecciones aprendidas, los requisitos y los factores clave de éxito para el diseño y la aplicación de un modelo de identificación y evaluación del riesgo operacional en una empresa de telecomunicaciones.

Conclusiones del estudio empírico

La principal conclusión del estudio empírico es la creación y el análisis de la aplicabilidad del modelo para identificar y evaluar los riesgos operativos de TELCO. Algunas razones justifican esta afirmación:

- Se ha podido obtener información relevante para desarrollar los modelos de identificación de riesgos y la metodología de evaluación de riesgos para crear el modelo de identificación y evaluación de riesgos operacionales para TELCO.
- El modelo de identificación y evaluación de riesgos operacionales ha producido resultados consistentes con los esperados, al haber sido contrastado con los responsables de las unidades de negocio dentro del ámbito de la investigación.
- Las explicaciones e interpretaciones de la información recogida en cada una de las tablas de resultados empíricos aportan información operativa y de negocio para evaluar el riesgo y acometer las dos siguientes fases del proceso de gestión de riesgos (respuesta al riesgo y seguimiento y reporte). De hecho, la interpretación de las tablas de *outputs* (resultados empíricos) incluyen comentarios que, además de los resultados numéricos de la estimación de riesgos tras haber realizado el estudio de caso en TELCO, permiten deducir varias conclusiones sobre determinadas decisiones a tomar para la implantación del modelo de identificación y evaluación de sus riesgos operacionales y su tratamiento.
- Una de las primeras decisiones tomadas en el estudio de caso fue el nivel de la estructura organizativa al que se dirigirían los cuestionarios. La opción metodológica elegida, descendente (*Top-down*) y parcial, se ha revelado como la más adecuada para una empresa del tamaño y características de TELCO, en términos de impacto, tiempo, eficacia y a la vista de los resultados e información obtenidos.
- Otro aspecto importante en la ejecución del proceso de autoevaluación en TELCO ha sido la aplicación de los cuestionarios, es decir, los riesgos que afectan a cada unidad de negocio. Para ello, se realizaron varias

reuniones para preparar la ejecución de los cuestionarios, tal y como se explica en el diseño de la investigación.

- En cuanto a la gestión del riesgo operacional, el modelo propuesto y aplicado no sólo permite el desarrollo del ciclo de control de riesgos (identificación, priorización, medición y control de los riesgos operacionales), sino también el apoyo posterior en la gestión de los mismos (planes de acción y tratamiento de los riesgos).

En cuanto a **la relación entre las proposiciones y los resultados obtenidos** en el estudio empírico, podemos destacar lo siguiente:

- Los resultados del estudio empírico muestran que ha sido posible crear modelos para la identificación de los principales riesgos operativos de TELCO, el caso de estudio de una gran empresa del sector de las telecomunicaciones **(proposición 1)**. A partir de las herramientas metodológicas de investigación para la recogida de datos (principalmente, sesiones de *brainstorming* y entrevistas semiestructuradas apoyadas por cuestionarios), se han podido identificar los eventos (clasificados en diferentes grupos de tipos de riesgo), los factores de riesgo y los marcos de efectos del riesgo (pilar de identificación del riesgo operacional) para TELCO. La información se detalla en varias tablas. Estos resultados fueron contrastados por los directivos de TELCO, que finalmente confirmaron su validez, tanto en lo que se refiere a su estructura como a su contenido específico y a los ejemplos que evidencian los eventos.
- Por otro lado, estos resultados empíricos muestran el desarrollo de una metodología para la evaluación de los riesgos operativos identificados para TELCO **(proposición 2)**. Tomando como punto de partida los riesgos identificados y aplicando la metodología de investigación descrita, fue posible desarrollar el proceso y el método de evaluación de riesgos operacionales que conforman el marco metodológico de evaluación de riesgos operacionales. Esta metodología se aplicó para cada unidad organizativa en el ámbito del estudio de caso de TELCO, en el que los principales directivos fueron informantes clave para la recogida de datos. Se realizó un análisis cuantitativo de las estimaciones subjetivas, cuyos *inputs* fueron el impacto económico y la probabilidad de ocurrencia de cada evento para calcular las pérdidas esperadas, inesperadas y las clases de calificación para la evaluación del riesgo. Los resultados empíricos se muestran en las tablas incluidas en la sección de análisis de resultados. Los resultados numéricos, cuya interpretación se describe, fueron analizados

conjuntamente con los directivos de TELCO para concluir que se trata de una información práctica y ajustada a su experiencia sobre la medición de cada riesgo.

- Además, es una información muy útil para la toma de decisiones sobre el tratamiento de los riesgos y los planes de acción. De hecho, una vez identificado y medido el riesgo operacional de TELCO, se pueden considerar tres opciones principales para el tratamiento del riesgo (se ha omitido la opción de evitarlo o eliminarlo): mitigar los riesgos (acciones mitigadoras), transferirlos (por ejemplo, contratación de seguros o actividades de *outsourcing*) o aceptarlos (incluirlos en los presupuestos anuales). Esto se describe en el marco del proceso de gestión de riesgos.

En definitiva, la conclusión más relevante del estudio empírico es que **se han podido contrastar las proposiciones específicas** de la investigación, vinculando los datos a las proposiciones de la investigación. Los criterios para la interpretación de los resultados están contenidos en la creación del propio modelo, tanto para los eventos identificados de TELCO como para la metodología de evaluación del riesgo operacional. Asimismo, la verificación de estas proposiciones responde a los objetivos de la investigación y a las preguntas asociadas.

Principales contribuciones

El análisis de los resultados proporciona una comprensión significativa del modelo de identificación y evaluación del riesgo operacional propuesto y su aplicación práctica, por lo que ofrece varias **contribuciones teóricas y de gestión e implicaciones prácticas**.

La investigación contribuye a nuestra comprensión teórica del tema (ERM) a varios niveles. En primer lugar, el estudio propone un modelo innovador de identificación y evaluación del riesgo operacional basado en modelos ERM universalmente aceptados. En segundo lugar, en lo que respecta a la evaluación del riesgo, la investigación tiene en cuenta experiencias probadas y sólidas del sector financiero y de seguros (por ejemplo, el enfoque de distribución de pérdidas). En tercer lugar, dado que las etapas de identificación y evaluación de riesgos son fundamentales en el proceso de gestión de riesgos, la investigación ofrece un enfoque práctico para la aplicación de la ERM basado en los conceptos teóricos incluidos en las diversas normas y modelos de gestión de riesgos. En este sentido, la aportación de este trabajo se basa en la creación (construcción) y aplicación efectiva de un modelo de identificación y evaluación de riesgos operacionales para TELCO que permita establecer, como "mejor práctica", la

implantación de modelos de gestión de riesgos operacionales, totalmente alineados con los modelos (COSO) y normas (ISO 31000) comúnmente aceptados en esta materia. En cuarto lugar, una vez que TELCO ya disponga de datos históricos como resultado de esta investigación, el modelo de identificación y evaluación del riesgo operacional desarrollado en este estudio facilitaría el desarrollo de un proceso de captura de datos de eventos de pérdida (LDC-*Loss Event Data Capture Process*) que debería ser capaz de identificar, validar y obtener resultados sobre las pérdidas operacionales de manera fiable, garantizando: (i) la integridad de los datos registrados; (ii) la accesibilidad de la información registrada; y (iii) la calidad y cantidad de la información registrada.

La investigación también tiene varias contribuciones en materia de gestión. En primer lugar, dado que las organizaciones tienen que centrarse en el desarrollo de prácticas de gestión de riesgos para identificar y evaluar sus riesgos operacionales, el modelo propuesto es un enfoque práctico para lograrlo para la industria de las telecomunicaciones, donde hay una falta de literatura e investigación. En segundo lugar, las empresas de otros sectores, aparte del financiero, el de los seguros y el de las TELCO, pueden extrapolar el contenido de esta investigación para identificar y medir sus riesgos operacionales utilizando modelos de identificación de riesgos y metodología de evaluación de riesgos (proceso y método) robustos y contrastados. En tercer lugar, los resultados implican que existe un impacto fuerte y directo de las prácticas de gestión de riesgos en el rendimiento de las empresas, ya que los riesgos operacionales que pueden ser identificados y evaluados, son clave para el negocio. En cuarto lugar, en cuanto al proceso de LDC basado en el desarrollo del modelo de identificación y evaluación del riesgo operacional, contribuiría en la: (i) la creación de una cultura sólida en la organización mediante la implicación de todas las unidades de negocio en el proceso de LDC y la definición y difusión de una metodología única y común de registro de riesgos; (ii) la formalización del proceso de LDC (identificación, validación y reporte); y (iii) la implantación de un proceso dinámico que pueda actualizar las fuentes de información y reflejar con precisión la exposición de la empresa a los riesgos operacionales en función de la evolución de la organización. En quinto lugar, el estudio puede ser apreciado por los directivos para contrastar sus conocimientos previos sobre el impacto del riesgo operacional; de hecho, las organizaciones más destacadas se centran en aprender de los fracasos y en mejorar los procesos organizativos para la prevención de riesgos en el futuro, y un mejor rendimiento de la capacidad de respuesta en el presente, donde este modelo de identificación y evaluación de riesgos puede ser una "herramienta de gestión" relevante para el proceso de toma de decisiones.

Implicaciones prácticas

Además, existe un doble conjunto de implicaciones prácticas: implicaciones empresariales e implicaciones para investigadores y profesionales. En cuanto a las implicaciones empresariales, los resultados de la aplicación del modelo de identificación y evaluación de riesgos fueron contrastados con los gestores empresariales de TELCO que confirmaron su fiabilidad y utilidad para sus procesos de toma de decisiones. Este trabajo de investigación ayudaría a las empresas de TELCO a conocer la utilidad y aplicabilidad del modelo propuesto para aportar valor a sus grupos de interés para: (i) obtener información relevante que permita a la dirección evaluar eficazmente las necesidades globales de capital; (ii) reducir las sorpresas y pérdidas operativas y mejorar las decisiones de respuesta al riesgo; (iii) gestionar los riesgos múltiples e inter-empresariales, considerando una gama completa de eventos potenciales, con el fin de aprovechar las oportunidades de negocio; y (iv) alinear el "apetito al riesgo" (tolerancia) y la estrategia. Otras implicaciones prácticas de este estudio están relacionadas con algunos beneficios de un modelo sólido de ERM y con el hecho de que los gestores de riesgos deberían abstenerse de centrarse únicamente en modelos teóricos, sino esforzarse por producir una identificación y evaluación de riesgos que pueda ser práctica para la toma de decisiones a fin de identificar resultados concretos. Las unidades de negocio y los propietarios de los riesgos deberían beneficiarse de tener una visión global de los riesgos, así como de analizar el perfil de riesgo de su actividad en condiciones adversas. La disciplina y la cultura del riesgo pueden promoverse mediante una contribución activa a la gestión del riesgo. Además, la aplicación de modelos de gestión de riesgos para las empresas del sector de las telecomunicaciones tiene como resultado la mejora de los procesos de toma de decisiones sobre los riesgos, posibilita las actividades de control, contribuye a la asignación eficiente del capital y los fondos de la empresa, y protege e incrementa el patrimonio de la empresa. El equilibrio entre el beneficio que aporta un determinado método y los costes que genera es el criterio básico para la aplicación de los marcos de gestión de riesgos en las empresas del sector de las telecomunicaciones. En algunos casos, la influencia externa, como la normativa regulatoria, puede afectar a la selección del método a aplicar en la gestión de riesgos.

En cuanto a las implicaciones para los investigadores y los profesionales, este estudio para la evaluación de los riesgos operativos podría servir de herramienta de referencia para otras entidades y sectores industriales, no sólo para los profesionales sino también para los investigadores. Los investigadores que sigan el camino descrito en este estudio podrían estar interesados en proponer marcos similares de identificación de riesgos

(OpRIF) y la metodología OpRAM para su aplicación en otras industrias y desarrollar casos de negocio para ilustrar la utilidad del enfoque. Esta investigación también podría contribuir a la comunidad académica en la consolidación de conceptos teóricos y un enfoque práctico para la disciplina de ERM. Por último, el estudio también describe futuras líneas de investigación, limitaciones e implicaciones para la gestión.

Finalmente, un último comentario "para reflexionar", como opinión personal, es que las investigaciones en materia de gestión de riesgos en las empresas de telecomunicaciones y tecnologías de la información suponen una "inversión" que merece la pena, ya que las actividades de estos sectores estipulan el funcionamiento no sólo de las necesidades de todo el sistema social, sino también de la vida de las personas, mejorando el estado del bienestar.