Ca' Foscari
University
of Venice

Master Degree
in *Management*

Final Thesis

Enterprise Risk Management and non-financial risks disclosure: The value of an integrated approach in communicating with stakeholders

Supervisor
Ch. Prof. Chiara Mio

Assistant supervisor
Ch. Prof. Silvia Panfilo

Graduand
Riccardo Linguanti
Matriculation Number 861798

Academic Year
2020/2021

A mia madre, per non aver mai dubitato delle mie capacità e per avermi sempre ispirato.

A mio padre, per essere stato la mia guida nel corso degli studi ed esempio d'integrità.

A mia sorella, fonte d'ispirazione, modello di tenacia e perseveranza.

A Matilde, per essere stata mia complice in questi anni e per aver sempre creduto in me.

INDEX

Abstract

The following thesis aims at examining in depth the relationship existing between enterprise risk management and non-financial disclosure.

Specifically, the first chapter focuses on a brief presentation of what is risk and how it can be classified, followed by a historical description of risk management, from the first silos approach to the always more integrated processes, expressing the need for business activities to pursue a more complete and exhaustive approach, which exploits opportunities deriving from risks and allows to manage them in a more integrated way. Successively the attention moves towards the theoretical description of ERM and its main peculiarities with a focus on the international framework provided by the Committee of Sponsoring Organizations of the Treadway Commission, with the objective of providing an effective framework for the implementation of ERM systems inside the organisation. The third chapter focuses more on the topic of non-financial risks, highlighting the effects on the financial performance of a company and the reason according to which this category of risks should be integrated with the management systems of all the other risks. Thereafter the composition analyses the topic of non-financial disclosure, remarking the importance of the transition from an "only financial" view to a more integrated approach to disclosure, which considers the interests of all stakeholders and, as a consequence, all the risks and aspects connected to non-financial issues.

Finally, in order to investigate whether companies with more sophisticated ERM systems and adopting a more integrated approach actually disclose to their stakeholders a greater level of information concerning their non-financial risks, the thesis through different case studies relates the level of ERM processes and the level of non-financial risk disclosure in a sample of Italian listed companies.

Introduction

For an organisation, risk management is a business process intended to manage risks faced by the company through systematic activities of identification, measurement, evaluation and processing.

In more detail, the most developed and innovative form of risk management is Enterprise Risk Management (ERM), which is defined as a cultural approach embracing a set of capabilities and practices that organisations integrate with their strategy-setting activity, with the aim of managing risk in the process of creating, preserving and realizing value. The main purpose of ERM is to protect and add value to the organisation to the advantage of its stakeholders, supporting the objectives set by the board through a consistent and systematic control of activities, enhancement of decision-making and planning of operations. ERM is an on-going and proactive process, which involves corporate strategy and which should be integrated in the organisation's set of values and culture, through a focused policy implemented by its managers, who empower individuals at all levels of the enterprise and make them responsible for specific roles and operations.

A holistic approach to risk management allows a company to take under consideration all potential impacts of the different types of risks on business processes, activities, individuals and services. More specifically, this study focuses on the relation between ERM and non-financial risks, including the debated and current topic of disclosure through non-financial reports.

Non-financial risks gained greater importance and esteem in the last two decades, especially if we consider the more frequent integration of non-financial issues inside programs of national governments and internal organisations. As a consequence, non-financial disclosure on environmental, social and governance topics became a fundamental moment during the activity of reporting, given the attention reserved to sustainable growth, in compliance with measures to preserve the environment and society's wealth. Part of the success obtained by an organization is attributable to non-financial risks management and disclosure, which enables consistency in the long term and gives the company a competitive advantage against other competitors. However, non-financial risk disclosure is the arrival point of a more complex process of reorganization of the company's strategy around the concept of integration and sustainability.

In fact, this paper aims at drawing attention towards the connection between ERM and non-financial risk disclosure inside large companies, referring to the exploitation of the opportunities represented by an integrated approach towards non-financial risks and to the importance of communication in terms of performance and business longevity. The study poses attention on one hand on the international frameworks provided to voluntarily embrace the culture of ERM approach and on the other, the establishment of initiatives at European level to shift non-financial disclosure from voluntary to mandatory. The research highlights the linkage among these topics, especially in the final chapter, in which an empirical study on some Italian listed companies is conducted to show the relationship between the level of implementation of ERM systems and the level of non-financial risk disclosure.

The results of this study actually demonstrate that large companies with a stronger ERM culture and more sophisticated approaches disclose to their stakeholders more information concerning the non-financial risks they face and how they plan to mitigate and manage these risks.

Chapter 1

From Traditional Risk Management to ERM

1.1 The relationship between risk and business

Conducting business activities means having to manage continuously changes in economic, environmental and social variables; and the way in which you manage these factors can lead the business to success or failure.

Among all the different definitions of risk given by economists and academics, one of the most recent ones, which gives a general definition of the concept of risk, is provided by the *Society for Risk Analysis* in 2018: "We consider a future activity [interpreted in a wide sense to also cover, for example, natural phenomena], for example the operation of a system, and define risk in relation to the consequences (effects, implications) of this activity with respect to something that humans value. The consequences are often seen in relation to some reference values (planned values, objectives, etc.), and the focus is often on negative, undesirable consequences. There is always at least one outcome that is considered as negative or undesirable."[1]

The main concept, which emerges from the words of the definition, is the idea of a double meaning of risk: a positive and a negative one.

In an economic-business like logic, risk is often seen as a potential damage as a consequence of a future event not aligned with the expectations; from this interpretation it appears clear that risk implies negative consequences, in other words risk may lead to an economic damage or a loss. However, the definition of risk provided by the SRA suggests that unplanned events may represent a threat or an opportunity for the firm. In this sense, the concept of risk assumes a meaning of neutrality, which has already been introduced in literature by Ulisse Gobbi who defined risk as "il campo estesissimo. Fra I due estremi della certezza dell'impossibilità e la certezza del verificarsi, in cui si ha, in varie gradazioni, l'incertezza che un dato evento si verifichi o meno"[2].

As previously introduced, business activities are characterized by situations of risk which are created and determined by changes in the internal and external environment and such alterations oblige managers to take decisions which could result in positive or negative

[1] SRA, Society for Risk Analysis, definition provided in the glossary, 2018.

[2] Definition provided by U. Gobbi, *L'assicurazione in generale*, Hoepli, Milano, 1898.

outcomes, especially for what concerns the ability of a company to create value. In order for the company to be successful and comply to its main purpose of perpetual continuation of the business, it is fundamental for its members to grasp the positive aspects of a sudden change and exploit the opportunities which come along with risk factors.

The different types of risks, which companies usually have to face, are generally identified according to the many different categorizations proposed by the literature. Among the many distinctions we find categorizations such as: exogenous and endogenous risks (the first ones arise from issues inside the company, instead the others originate from situations in the external environment on which the firm has no power to change the nature and dynamics), entrepreneurial and associated risks (this distinction originates from the value chain model of Porter, basically entrepreneurial risks derive from primary activities of the business, instead the others are attributable to secondary activities regarding collateral aspects of the firm), inherent and residual risk (the first category considers the impact of a negative event occurring without any internal control in order to manage and eliminate it, the second category analyses the significance of an event already occurred after having evaluated the effectiveness of internal controls designed to mitigate or eliminate such risk).

For the sake of the topic discussed in the thesis the categorization of risks, which is going to be taken into consideration divides risks into financial and non-financial. This distinction, not only is functional to our main topic and for our further analysis, but it is also one of the most recent classifications in literature, which better fits with modern issues.[3]

Financial risks are the most intuitive one to identify since they originate and are related to the typical and standard conduction of an economic activity; these risks are linked to the price of financial tools exchanged on the market, such as interest rate risk, exchange rate risk, credit risk, liquidity risk, inflation and the intrinsic risk of financial markets.

For the topic of the paper the category of non-financial risks is of greater interest. Non-financial risks include a substantial and significant list of risks, which are becoming always of greater importance, especially in the case of risk management activities. The most relevant risks pertaining to this category are the following.

Strategic risks refer to the extent of success of business strategies defined by the top management, which should consider events from the external environment and try to anticipate or manage potential risks connected to them. Among this specific risk we can identify R&D risk, customer risk, market risk or innovation risk.

[3] Distinction proposed by Professor S. Panfilo in "*La gestione del rischio e la sua comunicazione. Gap teorici ed evidenze empiriche nelle società quotate italiane",* pp. 17-19, Aracne, 2020.

Environmental risks refer to risks of the company in quality of entity operating in an environmental context and to the risk of damages caused by the firm itself to the environment. One of the most discussed and dangerous risk among these is the climate change risk connected to GHG emissions (greenhouse gas emissions).

Operational risk refers to typical business activity and the efficient use of resources, some examples are risk of fraud, governance risk, technological risks or risks linked to third parties in the supply chain.

Compliance risks are associated to the correct compliance with regulations and laws.

Social risks refer to those risks which the company may cause to the community, so not only employees but also society. A clear example could be the risks connected to an activity in a social environment or the case of the pandemics, which forced companies to deal with regulations and impositions in order to safeguard the health of people.

Reputational risks are linked to the image and the "name" of the company; often these risks are connected to other risks, since they derive from negative situations due to various reasons; in any case these risks contribute to the deterioration of the firm's reputation to the eyes of stakeholders and may influence negatively also performance.

This holistic view on the range of risks which companies have to deal with gives the idea of a continuous research and evaluation process in order to avoid dangerous and harmful situations. In order to identify, analyse and elaborate a strategy to mitigate or eliminate these risks, managers implemented risk management procedures, to simplify the "hedging" activity which the company should conduct in order to preserve its performance and value. Anyway, risk management has a long story, which evolved during the years in order to reach its actual status, that is also in constant flux, wit the aim of keeping up with the demanding need of companies to manage risks of various nature at the same time.

1.2 Risk management and risk hedging: "fear" of the numbers

Risk management has always been considered an activity aimed at providing protection against the potential negative consequences of events. In the book *Enterprise Risk Management,* H. Felix Kloman said, "Homo sapiens survived by developing "an expression of an instinctive and constant drive for defence of an organism against the risks that are part of the uncertainty of existence". This "genetic expression" can be construed as the beginning of risk management, a discipline for dealing with uncertainty."[4]

The quote above gives us the perception of the importance of risk management, which is a discipline innate in human beings and exploited even unconsciously sometimes. In an organizational context, such as the business one, risk management is fundamental: as we have already introduced, the activities conducted by a business are pervaded by risk, which in turn has to be adequately managed in order to guarantee a safe continuation of the activities.

Risk management, as we mean it in its latest sense, was born around the 50's in the US and identified a branch of social sciences aimed at studying mainly pure risks inside the company, from an insurance point of view.

At its beginning, the process of risk management identified itself in the concept universally intended as "Traditional Risk Management (TRM)". TRM focuses on the management of pure risks (for example operational ones or risks derived from safety issues) and financial risks (liquidity, credit) and related hedging instruments, which consist in the stipulation of insurance policies aimed at preventing and protecting the firm from the undesired event by transferring the risk to a third party (the insurer).[5] From this description provided by Damodaran and Roggi, we can grasp the idea that risk management consisted mainly in a defensive process, with the objective of minimizing potential losses in the short term. This TRM approach, developed between the 70s and the 80s, focused only on risks that could have been insured or hedged through financial instruments such as derivatives; the other types of risks were not taken under consideration because the main interest of companies was defining secure and conservative investment policies, minimizing probabilities of default.

According to this approach, companies established some processes for the analysis and the hedging of risks under an insurance logic, rather than a managerial one, forgetting totally the

[4] Kloman, H. F., *Enterprise Risk Management*, Chapter 2: A Brief History of Risk Management, p.19 – 29, 2011.

[5] Damodaran, A., & Roggi, O., *Elementi di finanza aziendale e risk management. La gestione d'impresa tra valore e rischio*. Maggioli Editore, 2016.

aspects related to the maximization of value, but focusing only on minimization of downside risk.[6]

The main consequence of this approach is that the way in which the company faces the single sources of risk is not integrated; this management of risks is defined "silo by silo" in literature, which means that the business unit threatened by a specific risk was the one accountable for the management of it. The main objective, once again, is the minimization of downside risk, no matter the involvement of neither the board nor the coordination with other divisions of the firm; the only goal was hedging from the negative impacts of risk.

Risk hedging through the traditional approach results effective in case the firm aims at protecting its activities from external threats, however the whole business remains in a static position without any chance to exploit opportunities deriving from changes or upcoming risks. The main limit of the TRM approach is represented by the last issue introduced: hedging instruments allow the firm to minimize the risk of eventual losses in case of unfavourable events, but at the same time eliminate totally any opportunity of gaining advantage or creating value from an alteration in the usual business activity.[7] Furthermore, the activity of minimization of risk is not a synonym of value maximization: hedging allows the firm to create value if and only if the costs needed to implement hedging activities are exceeded by the benefit deriving from them.

We must keep in consideration the fact that companies have not abandoned hedging activities and these haven't been substituted by alternative activities of risk management. However, it is important to underline the process of evolution faced by risk management, which allowed combining risk management activities with complementary activities that enable the firm to consider and exploit potential opportunities, or upside risk.

In fact, taking TRM as a starting point, the process of risk management experienced several changes, keeping in mind the limits of a traditional approach: risk is not considered anymore as a simple threat, but it starts to be considered as an opportunity and so companies start reasoning on an integrated way of managing risks, considering all enterprise risks impacting the business and not only financial risks.

Professor Daniel A. Rogers states: "Financial risk management strategies, often called financial "hedging," can be considered as a predecessor in the evolution of enterprise risk management

[6] Ibidem.

[7] Eiteman, D. K., Stonehill, A. I., & Moffett, M. H., Multinational business finance. Pearson Global Ed., 2016.

(ERM) programs. ERM addresses a far broader array of risks than those that can easily be hedged using financial contracts"[8].

[8] Rogers, D. A., Managing financial risk and its interaction with enterprise risk management. John Wiley and Sons., 2010.

1.3 A broader approach to risk: Business Risk Management

A narrow vision of risk led companies to embrace a more comprehensive view concerning the way of managing risks inside the business. This broader managerial approach aims at integrating the efforts of operating managers and risk managers; in fact business risk management approach doesn't consider risk as an event which has to be delegated to third parties such as insurance (this is the main braking point separating the TRM approach from the BRM one), instead dealing with risk and its consequences becomes "part of everyone's job"[9] in the firm.

Over the years during the 90's the evolution of traditional risk management focuses on the optimisation of business performance. The reason moving companies towards this intention derives from the fact that in those years many risk incidents in non-financial areas constitute the main reason of underperformance for firms. The frequency of these incidents pushed managers and their boards to increase awareness towards the many different type of risks, not addressed by traditional risk management, which can negatively condition performance. Even though the "discovery" of these unconventional risks represented a threat for firm's management team, executives quickly realized that these risks deriving from non-financial areas were not properly managed, however it was perfectly possible to manage them more effectively.

From this consideration, the risk management system of firms evolved from a traditional approach to a more sophisticated one, known as business risk management; the transition occurred through the implementation of a more systematic risk evaluation process: accountability for specific risk areas were assigned to appropriate managers and the main risks, identified as critical to the firm, were approached through verified risk management processes.

It is too simple and reductive to define business risk management as an evolution process from traditional risk management, which allowed companies to manage risks other than financial. Contextually to this transition firms initiated a process of progressive integration in the management of the different types of risks, and started to rationalize techniques of recognition and transfer of risks with the aim of limiting downside aspects, but more important with the goal of exploiting opportunities which could have enhanced performance. This new vision towards risk denotes an additional change besides the new approach in the management of the different types of risks; the nature of this variable starts to move from a

[9] Citation by Microsoft's Jean-Francois Heitz, taken from *Enterprise-Wide Risk Management: strategies for linking risk and opportunity,* James W. Deloach, 2000.

completely negative connotation towards a "hybrid" one: risk starts to be seen as a "leverage to gain a competitive advantage, if well managed"[10].

James Deloach claims that with a business risk management approach firms increased the sophistication of both treasury and insurance functions, not only to manage financial risks, but also to broader strategic issues. At the same time, this new way of interpreting risk means that risk managers and operating managers have to make an effort in working together and trying to individuate the source of risks. To this end, Professor Chris Wasden said, "The risk managers need to understand the business; the business managers need to understand risk- so much so that risk and business management become indistinguishable"[11].

From this citation it seems clear that the new frontier of risk management is devoted to evaluation of upside risks (opportunities deriving form risk itself) and integration between risk management and strategy; however in this phase the focus is still on individual risks or group of risks connected between each other.

[10] Translation from S. Panfilo, *"La gestione del rischio e la sua comunicazione: gap teorici ed evidenze empiriche nelle società quotate italiane",* p.25, 2020.

[11] Professor Chris Wasden is the Executive Director of the Sorenson Centre for Discovery & Innovation at the University of Utah.

1.4 Creating value upon risk through a new source of opportunities: ERM

At the beginning of the new millennium the evolution of risk management moved towards an integrated approach in the management of the different types of risks. The idea of a defensive logic with the goal of reacting to events caused by sources of risk will be abandoned in favour of a more proactive approach directed towards the enhancement of business performances. The growing dynamics and competition inside the context of businesses and the lack of consistency across the firm in terms of details, managerial methods and guidelines cause many issues to executives in the recognition and evaluation of risks in terms of aggregate effects on the whole of the business.

This new way of managing risk is defined in literature as Enterprise risk Management approach (ERM) and its main goal consists in elevating the importance of a transversal and integrated vision of risks inside the general frame of the company. ERM, with respect to the positive steps forward of BRM, takes additional steps to raise the value proposition of the company to a higher level, trying to adopt a strategic vision of risk management in which risks are considered and evaluated in terms of overall impact on the firm, in the short and long term period.

ERM retains the original focus of TRM on reducing loss exposure to the minimum level, however it tries to foster management confidence through a systematic approach that identifies all of the enterprise's risks and tries to support resource allocation through a rigorous procedure of risk prioritization. In other words, ERM's goal is to create a disciplined and well-structured process in order for the company to be in the best possible position to take crucial decisions concerning the strategic aspects of the business.

The key element of difference with BRM, which sets off the evolution in risk management, is the engagement with al business units and the distribution of responsibility concerning risk management. We do not talk anymore of a firm's division whose job is to identify risks and deal with them; ERM is an activity part of the business culture, which is of interest for each unit.

As we have already highlighted, ERM allows the company to grasp the upside risk and exploit the opportunities deriving from potential threats, but it also allows mitigating the downside risk; overall the management process ends up in an approach enabling managers to choose the best strategy. As Holderbank CEO Thomas Schmidheiny said "This is not the elimination of risk, but rather, it is an unparalleled tool for strategic planning and control"[12].

[12] Citations from J. Deloach, *Enterprise-Wide Risk Management: strategies for linking risk and opportunity*, p.23, 2000.

The evolution from BRM to ERM is not so simple and instant to understand: as anticipated above, an enterprise deciding to adopt an ERM culture should be proactive, anticipatory, dynamic and must support the business model in the value creation process. The new interpretation of risk management is obviously concerned with hedging from risk exposure, but it is likewise interested in betting against risk consistently with the business objectives and strategies. If an organization is willing to create a competitive advantage by integrating risks across business unit and taking risk management to a strategic level, it must "raise the bar". The key is to implement an approach aligning strategy, processes, culture, know-how and performance, in order to optimize results for the firm at each level.

Based on the perspective of the thesis, it is important to underline that the primary purpose of ERM is value creation for stakeholders; such aim is reached through the enhancement of capital efficiency, allocating resources in an objective way and identifying connected risks and potential effects on the company's performance, by supporting decisional processes based on information determining which variables have a negative impact on the company and risky situations which can lead to a potential competitive advantage[13].

Michel Crouhy said "an ERM system is a deliberate attempt to break through the tendency of firms to operate in risk management silos and to ignore enterprise risks, and an attempt to take risk into consideration in business decision much more explicitly than has been done in the past"[14].

It is clear, also from these words, that ERM is not only an activity to be implemented in the management of a firm, ERM is a way of interpreting management meant to improve the organization as a whole and to integrate all business levels and units, so that each one is responsible for its risks, but different areas are not separated by each other, quite the opposite, business units work together in order to manage the risk in the most effective way, trying to gain the greatest possible advantage for it, exploiting any potential upside opportunity deriving from the issue taken into account.

[13] Interpretation of ERM explained by P. Tarallo, *La gestione integrata dei rischi puri e speculativi,* 2000.
[14] M. Crouhy, D. Galai, R. Mark, *The essentials of risk management,* p.15, 2006.

1.5 An alternative approach to risk management: the road towards ERM

There is an alternative description, beyond the steps described above, of the evolution in risk management approaches which led to the success of ERM. It is very difficult to give one specific definition of risk management and provide a unique process through which ERM has been reached; also because in literature we find plenty of frameworks describing risk management. The intent of the paragraph is to provide a synthetic description of the main approaches to risk management, providing a logic path which laid the foundations for the modern ERM approach, trying to highlight the techniques adopted by companies in managing risk. To pursue this objective we're going to take into consideration the categorization proposed by Professor Paolo Prandi in *"Il risk management. Teoria e pratica nel rispetto della normative"* (2010).

As it has been already pointed out, ERM is an integrated risk management approach, which observes risks from "the top" under a systematic vision, trying to consider all the existing relationships between different types of risks. This kind of logic abandons the typical "silo by silo" evaluation of risks and embraces a broader evaluation of risks which engages the whole of the business, giving birth to a true culture shared among all individuals in the firm.

The main differences between the approaches we are going to propose consist mainly in the business areas on which they focus, in the relevance of specific phases and in the objectives of each approach. The common aspects of these alternative managerial approaches, which brought to ERM, stands in the effect on the business' culture: risk management previous to ERM focused only on specific units of the firm and they do not foster a shared culture of managing risk in an integrated way.

The main alternative approaches that are going to be analysed are the following:

- Traditional Risk Management
- Financial Risk Management
- Project Risk Management
- Control Risk Management [15]

As we have anticipated, traditional risk management (TRM) is considered the closest ancestor to ERM. The implementation of this approach is characterised by four steps.

[15] This categorization of approaches and the following description are an interpretation of Professor Paolo Prandi, *Il risk management. Teoria e pratica nel rispetto della normative,* pp.192-197, 2010.

The first phase consists in the identification of risks that could potentially damage the firm; during this step the company tries to manage the information concerning risks faced, trying to organize a framework able to describe the risk profile to which the frim is exposed.

The second phase consists in the evaluation process of risks to which the company is exposed; during this moment an analysis of how to manage the different risks is conducted in order to understand the more convenient way to hedge business performance.

The third phase is the core of the TRM approach: the firm applies measures of prevention and of risk-transfer to third parties, which have been planned during the precedent phase.

The forth and last phase is known as "risk control"; it consists in the assessment of the results reached through prevention, managing and elimination of business risks.

Financial Risk Management (FRM) is an approach that focuses on a specific business unit: financial risks management. These types of risks may concern the operative area such as the financial one. FRM is a business function characterised by the willingness to ensure an optimal allocation of business capital, guaranteeing an adequate remuneration in the long run according to specific conditions of risk accepted by the executives. The main phases to be followed by the management in implementing a FRM approach are briefly described in the following paragraphs.

First of all managers should identify all possible scenarios which could verify and define a time span.

Secondly, executives should determine cash flows from assets and liabilities trying to classify them according to type and commitment in order to pursue the match between assets and liabilities.

Finally, managers should make an effort to forecast future interest rates and cash flows through the implementation of statistic-financial techniques, which analysis and evaluation is objective due to the availability of past data collections.

From the operative point of view, the previous analysis allows identifying several analogies with an integrated risk management system, however it is clear that this type of risk management approach focuses exclusively on a single business area: the financial one.

Project Risk Management (PRM) arises with the aim of managing risks connected to the realization of big projects characterised by the presence of a clear and well-defined plan. The approach towards risk offered by PRM is mainly defensive, due indeed to the nature of this risk management approach, since PRM activity focuses on identifying, evaluating and possibly eliminating any threat potentially damaging the outcome of the project.

A further approach to risk management is proposed by Control Risk Management (CRM), which can be defined as a managerial activity aimed at guaranteeing, with a consistent reliability, the correct development of the business activities according to existing procedures, risk appetite and regulations defined by the firm itself. Basically CRM is a defensive tool, which assesses and measures potential gaps between existing rules and business activities. CRM assumes different implications according to the subject to which it refers and according to the subject having the role of monitoring the activities in compliance to regulations and plans defined by the company.

Three situations can be identified according to the previous premise.

CRM may be defined as a corporate governance tool, which allows shareholders to assess whether the company and managers are following the road traced by them, pursuing the goals set. CRM approach could be identified as a guideline and assessment tool for executives, since it allows managers to verify if subordinated units are operating according to the guidelines provided by the company. Furthermore, CRM could also act as a guarantee, certification and communication tool for stakeholders: these subjects can verify whether the economic activities pursued by the company are damaging their interests or not.

As a conclusion to the previous analysis of the evolution of risk management, it is undeniable to claim that risk management represents a turning point in the activity of business management, since it allowed opening the mind towards alternative ways of managing risk and hedging from unknown events different from insurance. During the years different theories and approaches dealt with this issue in different ways; in a second moment, the evolution of the concept of risk, a more systematic and long-term oriented vision of the concept of business allowed the traditional techniques to evolve towards a more sophisticated and transversal method known as Enterprise Risk Management. Once again, there is no date defining the birth of ERM as a new disruptive approach in risk management theory; what is obvious is that the implementation of an integrated approach to risk management is more than an opportunity for the world of companies; nowadays it has become a necessity.

Chapter 2

ERM and the initiatives to provide an international guideline illustrating how to conduct the activities of risk management

2.1 Enterprise Risk Management: the features of an integrated approach

In literature there are different interpretations and definitions on the theme of enterprise risk management, the reason of this variety of explanations is partially due to the complexity of the topic and also to its eclecticism in terms of application to business activities.

Indeed the definition of ERM, which established the most worldwide, is the one provided by the Committee of Sponsoring Organizations of Treadway Commission (COSO) in 2004 "Enterprise risk management is a process, effected by an entity's board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within the risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."[16]

From the definition above it is possible to grasp the concept of integration, in other words the evaluation of processes and strategies across all of the enterprise, involving the whole of the business. The engagement of all business units and people working within the enterprise is recognised as an essential aspect to gain a competitive advantage and reach the goals set. Committee of Sponsoring Organizations of the Treadway Commission (COSO) is an American organization founded on cooperation, which established in 1985 from the initiative of five entities representing different categories such as internal auditors, accountants and professionals working in finance. In addition to the job of favouring ERM implementation, the Commission is also in charge of defining frameworks dealing with the activity of internal control and prevention of frauds inside the business.

The explanation provided by this entity is not "accidental", neither it can be considered as one of the many definitions of ERM, which can be found across existing literature. This definition of ERM is included in the document published in 2004 by the Commission itself *"Enterprise Risk Management – Integrated Framework"*, in which the fundamental elements of ERM are identified and presented. The following paragraphs of the chapter are going to analyse in

[16] Definition provided by COSO, "Enterprise Risk Management: executive summary", www.coso.org, 2004.

deeper details what are these elements, why they have been identified as essential in risk management processes and how they have changed since 2004 in the latest publications of the Commission.

This definition of enterprise risk management and the framework presented by the COSO allowed third parties to make some considerations regarding the framework and the nature of ERM; in particular way a very interesting analysis has been conducted by Associazione Italiana Internal Auditors and PwC in a volume published by the Italian newspaper Il Sole 24 Ore. Some key aspects and elements of ERM have been highlighted and analysed; in order to give a wider perception of enterprise risk management and its implications, we're going to report these features.

First of all, ERM is an on-going and pervasive process involving all members of the enterprise: this is not a stagnant activity with a single function, ERM is a series of subsequent actions taken by the management and related between each other, in the interest of the company. It must be clear that enterprise risk management is not an additional activity to add to the existing one, it is a discipline invading all business units and evaluating all interconnections among them. Since it is a process which involves each division of the business, in the same way it involves all members of the firm: from the top management to simple employees, without any exclusion. The process of risk management is carried out by all of the people inside the firm; individuals' experience, attitude and vision shape, but at the same time is influenced by, the process of risk management, in order for people to understand what type of risks the business is facing. For a correct implementation of an ERM process, it is fundamental that people understand their position, what they are expected to do and what are the goals and the vision of the company; if people know what is their role and what they are held accountable for, then it will be easier to approach to business risks in the correct way, following the strategy set out by the company.

The publication cited above talks about strategy because ERM becomes essential also in strategy setting, especially in relation to the choice of the best alternative according to the risks which could be faced by the firm. The relation between strategy and ERM is so important because strategic goals define specific goals of each unit, for this reason ERM reveals crucial for managers in determining targets, which are coherent with the mission and vision of the company and which keep into account the risks the firm will run into.

In order for ERM to be effective, it should be implemented at every level inside the organisation, so both at unit level in conducting single activities and in general (when setting goals, strategy planning…). This holistic approach allows the company to consider the entire

risk faced by its activities; each individual accountable for a specific procedure or outcome should provide an opinion concerning the type of risk and the level of risk the firm is going to incur, once the management gathers all of the information required it is easier to determine if the overall risk is consistent and coherent with the risk appetite of the company. The fact that risks should be evaluated in a systemic perspective must be stressed: only a general and complete view of the level of risk incurred gives the possibility to managers to decide whether it can be accepted or not. The way in which risks are interconnected between each other is the key in enterprise risk management, because the risk faced by a single unit may be excessive compared to the level of acceptance, however in the broader context of the business this risk could be compensated by a positive effect on another unit, which mitigates the initial one. In simple terms: overall risk must be aligned with the firm's risk appetite.

In the perspective of alignment with risk appetite, ERM is planned in order to prevent potential threats, which could interfere with the activities and exhibit the firm to a risk greater than the acceptable level. Obviously this threshold varies according to the type of business and according to managers, however, whatever the risk appetite, the aim of ERM is to provide a series of processes able to allocate resources among units in order to mitigate risk and keep it under the desired level.

ERM enhances the chances of the firm to reach its objectives. The definition provided by COSO states "…provide reasonable assurance regarding the achievement of entity objectives". It is impossible to predict the future with certainty, however an ERM approach gives the opportunity to reach with greater chances the objectives set by the management according to its risk appetite.

Essentially ERM processes aim at reaching targets and goals set by organisations, so adopting an ERM approach means implementing a system which enhances the chances of being successful. "ERM is a mean with an end, not an end itself"[17].

This brief analysis on ERM gives us the idea that integrated risk management doesn't have the simple aim of setting itself as a model for risk management, at the most it implies a proper cultural approach which shows itself concretely under a managerial logic, which penetrates into the company and into each individual. Implementing an ERM approach ensures a pragmatic support in terms of proactive reaction to external events and effective decision-making, which is necessary to manage efficiently the core business, avoiding delays or issues

[17] Translation from *La gestione del rischio aziendale, ERM – Enterprise Risk Management: modello di riferimento e alcune tecniche applicative*, Associazione Italiana Internal Auditors (AIIA), PricewaterhouseCoopers (PwC), Committe of Sponsoring Organizations Treadway Commission (CoSo), Il Sole 24 Ore, 2006.

cause by exogenous factors. The adoption of this model should be perceived as a tool facilitating the development of all business activities, inside and outside the firm. Above the creation of a shared culture among the members of the company, ERM adoption also enhances relationships among stakeholders, since a greater control over risks translates into a greater solidity of the firm and a perception of consistency by the public.

2.2 ERM activity as a tool to mitigate and manage risks: advantages and oppositions

From its beginnings, ERM represented a disruptive approach and a very useful tool if we consider all of the risk management systems implemented before it. The paragraph above drew attention to some of the main aspects and implications of ERM, taking as a starting point the words of the definition provided by COSO in its first framework; at this point the focus moves towards the different peculiarities and main characteristics of the implementation of an ERM approach, trying also to point out some of the advantages of the adoption of such a system but also some limitations perceived by professionals and businesses.

There are five main aspects to point out considering ERM system:

- ERM takes into consideration all risks pervading the company
- Risks are managed through an integrated approach embracing all issues
- Broad vision of all types of risks
- ERM is long-term oriented and focuses on stakeholders
- ERM's goal is to create a structure suitable for risk management

In the initial analysis on the "history" of risk management it has been stressed the fact that at the beginning companies focused only on pure risks, only in a second moment they started taking under study the single risks of each unit, trying to mitigate the downside risks. Part of the innovation in implementing an ERM system stands in the evaluation of pure risks and speculative risks, so basically risks which can translate into a positive outcome for the firm if managed in the correct way. In general, ERM considers existing risks for the company but also potential ones, which could verify in the future. It is of vital importance for an ERM system to be successful to consider and assess all types of risks potentially dangerous for the performance of the business. Ignoring some risks or a poor identification of them can lead to an incorrect allocation of resources and effort, exposing the company to a greater risk. In "Corporate Value of Enterprise Risk Management the next Step in Business Management" Professor Sim Segal states that many companies are convinced of implementing an ERM approach, even though their attention is focused chiefly on financial risks, without any attention on the management of strategic and operational risks. The main cause of this shortcoming stands in the attitude of the management, which many times is unable to quantify and measure strategic and operational risks or often acts under a perspective strictly financial. According to Professor Segal, the inability of measuring strategic and operational risks lies in the lack of frameworks and models used to quantify the risk and in the lack of objective data and information, which allows evaluating scientifically the situation. Obviously, strategic and operational risks depend strongly on the type of business and activities

conducted, however the analysis of all possible scenarios as a consequence of a sudden event allow managers to consider and evaluate these risks in a more objective way. Also the abuse of financial perspective represents a problem in the implementation of an integrated approach: too often people in charge of risk management duties are financial experts and their evaluations are biased by their "financial approach", which tends to consider financial risks as the principal ones responsible for business failure[18]. In concrete, ERM is a strategic approach to risk management, which means that most of the efforts must be oriented towards risks representing the greatest threat to the business.

Approaching risks in an integrated way means involving all business units and all members of the organisation in the activity of risk management. A proper integrated approach to risk management implies systematic evaluation of risks and the adoption of a "group culture", where each activity is kept into account. It is not only about considering the relationships between risks and evaluating them, ERM should be proactive towards a specific risk but at the same time it should consider how the managerial strategy of risk hedging impacts other risks and their management.

ERM approach proposes a broader vision of risk with respect to the first systems of risk management such as Traditional Risk Management. As we have briefly introduced in the first chapter, TRM classified risk as a threat from which the firm should hedge itself, this means that companies considered only the downside risk or, more simply, the negative aspects. One of ERM's disruptive element is the exploitation of the upside risk, which means using risk as an opportunity to grow and create value for the firm. Considering also upside risk mark a step forward in terms of opportunities for the firm: the close link between risk and performance allow managers to implement decisions trying to avoid any type of risk but at the same time the company doesn't loose the opportunity to take a potential advantage from a situation (only apparently negative) which has created.

One of the reasons pushing a company to implement an ERM system is the long-term orientation. In the past millennium, as we have pointed out, the focus of managers was pointed mainly towards the financial area and short-term results: profit was the main goal. With the arrival of new vision and management systems, also goals and objectives of firms started to modify; in our case, when companies started to approach risk management through ERM systems, also their perspectives started changing towards a long-term view. Risks

[18] Professor Sim Segal describes such attitude as "Financial analyst bias" in *Corporate Value of Enterprise Risk Management: the next Step in Business Management*, Hoboken, New Jersey: Wiley, 2011.

apparently insignificant in the short-term could reveal dangerous and challenging in the long one, for this reason managers started thinking in a more critical way, trying to understand the implications of a risk which could potentially be faced by their company in the future. The characteristic of a long-term orientation comes along with a clear focus on all of the categories of stakeholders. Taken for granted that due to obvious reasons the main stakeholders in most firms are shareholders, an interesting fact of ERM systems is that their implementation not only helps the business to carry out its activities more easily and more efficiently, it also allows to satisfy all other stakeholders pursuing their interests. The main objective of a business is to create value for its stakeholders, however threats, represented by risks of all kind, endanger the process of value creation because they can cause poor performance and in the worst cases failure. An ERM system works in the correct way if it gets harmonized with risk capacity and risk appetite of the firm: risk capacity is the maximum amount of risk the company can absorb and risk appetite is the risk the company is willing to accept in carrying out its activities[19]. The implementation of such risk management system imposes the management to evaluate very carefully all of the options because a small risk capacity and a great risk appetite may result in failure, on the other hand a great risk capacity but a poor risk appetite could reveal a huge lost of opportunities and, as a consequence, a huge loss of value for stakeholders. When a company adopts an integrated approach to risk management, it means that the main will is to maximize value creation, taking also advantages from potential risks.

The last point of our analysis underlines the fact that adoption of ERM systems implies the implementation of systematic approaches inside the company, which allow managing risks in an integrated way. According to Professor John J. Hampton, in order to reach the systematic approaches mentioned above, companies should implement a decision support system finalized at simplifying the job of all members of the firm managing risk[20]. Such decision support system mentioned by Hampton takes the name of "ERM Knowledge Warehouse": IT data storage containing all information concerning risk management activities of the firm. The aim of this storage is to support management's decision making by making available all the information regarding risk management activity of each business unit, processes and mechanisms used to prevent damages and past experience and data to improve the general managerial approach inside the business. The sharing of information helps to identify who is

[19] Description provided by COSO in *"Enterprise Risk Management: aligning risk with strategy and performance",* pp.53-54, June 2016 edition.

[20] John J. Hampton, "*Fundamentals of Enterprise Risk Management: How Top Companies Assess Risk, Manage Exposure, and Seize Opportunity",* American Management Association AMACOM, 2009.

accountable for a specific risk, since each category has a unit and an individual responsible for it. The adoption of a Knowledge warehouse implies also the redaction of a risk report, which includes all information concerning business risks in order for managers to evaluate levels of risk exposure of each unit, according to the firm's risk capacity. The objective is always trying to understand promptly where is the problem, who is responsible for it and how the risk can be managed quickly in order to avoid losses or, even better, in order to change the events and gain an advantage from the situation.

As a brief summary of the peculiarities of ERM, this last part of the paragraph is going to present some of the main advantages deriving from the implementation of such risk management system.

ERM allows a firm to align its strategy and its risk appetite; once the firm has determined its risk appetite, it evaluates and decides which strategies to implement and, as a consequence, it determines objectives and risk management mechanisms.

Implementing an integrated system of risk management also gives the possibility to the management to enhance the ability of recognising potential risks, evaluating them and produce strategies and process to react to them efficiently. In this way, undesired accidents and consequent losses can be dramatically reduced in favour of a more consistent performance.

The main characteristic of ERM approach is the inclusivity of all business units inside its managerial structure, which means that managers are provided with information concerning all business activities and related risks. The whole of these pieces of information and the chance to use them in risk evaluation process allow the management to understand precisely which are the financial requirements of the firm, under a view of optimization in capital allocation.

The systematic integrated approach characterising ERM ensures that companies provide unique responses to multiple risks, which means that one risk threatening a single business unit is not evaluated singularly, instead it is related to other risks existing in the firm. In this way it is more probable that a group of risks originating from different business units find a unique solution, reducing hazards, management and intervention costs.[21]

Connected to the point above, ERM approach also helps in the optimization of resources usage in risk management; above all resources of time, which are actually saved since the

[21] Associazione Italiana Internal Auditors (AIIA), PricewaterhouseCoopers (PwC), Committe of Sponsoring Organizations Treadway Commission (CoSo), *La gestione del rischio aziendale, ERM – Enterprise Risk Management: modello di riferimento e alcune tecniche applicative*, Il Sole 24 Ore, 2006.

continuous monitoring of potential issues and a 360 degree approach allow executives to manage risks when they arise, creating a proactive business environment.

"The very process of identifying risk can stimulate thinking and generate opportunities as well as threats." These words from Chapman explain that taking into account all events potentially impacting the firm, without focusing only on risks to which the company is exposed, puts the management in the condition of identifying not only risks but also situations which could potentially generate value for the company.[22]

ERM systems improve the solutions in response to the different risks identified. This approach provides the tools to evaluate whether it is convenient to avoid, reduce, share or accept the risk taken into consideration. This way of managing risk results more efficient due to the systematic approach in which all activities in the firm are kept under control and managed through one single broad managerial system, exploiting interactions among risks and eventually reducing costs of management.[23]

As a direct consequence of ERM implementation, an intuitive but also relevant advantage consists in the reduction of agency costs related to information asymmetry between managers and shareholders (but also stakeholders in general). A systematic and integrated approach to risk management translates into an improved communication with shareholders and parties involved in the business activities; for this reason access to credit results easier and evaluation from analysts and investors result more precise and effective.[24]

An ulterior benefit arising from ERM derives from disclosure. Even though this topic is going to be analysed and described in detail in the following chapters, it is important to underline the importance of the disclosure activity, which communicates information to the external environment (stakeholders in general) and to the internal one, with the aim of providing all the necessary data to guarantee a correct implementation of the risk management model.

In contrast to all the positive aspects of ERM systems and the advantages, which arise from the implementation of such approach, the following considerations point out some of the oppositions raised by managers against ERM approach. Even though ERM is an innovative model effectively enhancing performance, it is also characterised by some limitations, which make the implementation difficult. The main oppositions to ERM are the following[25]:

---

[22] Chapman R. J., *"Simple tools and techniques for Enterprise Risk Management",* John Wiley & Sons, 2006.

[23] P. Prandi, *Il risk management. Teoria e pratica nel rispetto della normativa,* Franco Angeli, 2010.

[24] Liebenberg A. P., Hoyt R. E., *"The determinants of Enterprise Risk Management: evidence from the appointment of chief risk officers"*, Risk Management and Insurance Review, Vol. 6, No. 1, pp. 37-52, 2003.

[25] The paper takes into consideration the analysis conducted by Beasley M.S., Branson B.C., Hancock B.V., *"ERM: Opportunities for Improvement",* Journal of Accountancy, vol.1 September, pp. 28-32, 2009.

- Core business and competition should have priority
- Economic and time resources are insufficient
- Management lacks competences
- Such activity does not add a consistent value to the company
- Perception of a lot of bureaucracy behind ERM implementation
- Regulations represent a tough barrier.

These doubts arise from the lack of perception of all benefits deriving from ERM systems and secondly difficulties such as shortage of resources or lack of competences emerge.

The main issue observed by most companies is linked to the high costs of implementation implied in the creation of a complex structure of monitoring and communication. Furthermore, management teams are reluctant in implementing ERM systems due to the massive time effort needed in the initial phase, even though, once started, ERM becomes a crucial tool in management with a significant saving of time and costs.

An ulterior problem, which could impede the ERM approach to risk management and discourage managers, is represented by the coexistence of multiple cultures inside the firm without a unique guideline of core values and beliefs shared by all members of the firm. In many cases firms own branches in different countries, which implies the presence of different cultures and languages according to the location of the plant. In order to reach an integrated approach to risk management and fulfil the objectives set by the management, the feedback concerning the response and interpretation of rules and behavioural regulations by different culture becomes crucial. The incorrect fulfilment of a procedure or activity conducted by an individual, due to a distorted perception of directions imposed by the central management, could invalidate the whole system, as a consequence the successful outcome of risk management activities and in turn the failure in meeting performance goals.

Despite the oppositions and resistances, in different cases the implementation of ERM has been promoted by the intervention of external financial or governmental bodies, requiring a more detailed and accurate analysis on the risks faced by the organisation. The fact that different authorities imposed limits and obligations safeguards more stakeholders of the companies, because such impositions in terms of adoption of risk management systems avoid, or at least mitigate, the negative effects of unexpected or underestimated risks, which in the worst cases cause failure and consequential losses for investors and stakeholders in general. Furthermore, an external imposition encourages firms to adopt and implement the model in a correct way, because they're going to be subject to controls and audits by the authorities, favouring further stakeholders safeguard.

All the doubts and complexities presented by an integrated risk management model can be partially overcome by a gradual introduction and implementation of the system; in some cases, it can be useful to identify the most critical risks to which the firm is exposed and address them initially, in a second moment such system can be expanded to the whole of the firm embracing all risks. Or, as an alternative, the implementation can start from one single business unit and progressively expand to all the business.

2.3 COSO framework from 2004 to 2017 edition: a revision of the approach to risk management

International institutions and organisations involved in risk management developed in last decades different standards with the aim of clarifying and formalising more precisely the process of risk management, in order to fulfil the need of risk integration in the complexity of business governance.

Standards in general are tools creating guidelines for the basic principles of the process, without taking away from enterprises the possibility of adapting those principles to their own organisational structure and situation. Each standard defines more or less a general approach to ERM, which means that it provides a framework as point of reference. A framework is a blueprint providing a guideline and a broad vision on the activities connected between each other, with the objective of simplifying the approach towards the realisation of a specific goal. In this specific context, the existence of a framework favours the implementation of ERM, since it presents a group of specific activities functional to the organisation and the definitions connected to such activities, which help in defining the system of risk management.

Even though there are lots of standards existing nowadays, the ones most diffused, which received greater success are ISO 31000 framework and the ERM framework proposed by COSO.[26] In particular, the framework that received most success and is most adopted worldwide is the ERM framework developed and published by COSO, for this reason the following considerations and the entire thesis will take this framework as the one of reference.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a joint initiative of five private sector organizations and is dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management, internal control and fraud deterrence. This risk management organisation works to improve the quality of financial communication through business ethics, efficient internal control systems and corporate governance. COSO is well-known for having developed initially in 1992 the *"Internal control-Integrated Framework"* report, which is an integrated manual with the aim of supporting organisations in the development and improvement of internal control systems, with the objective of integrating such systems with processes, policies and

[26] KPMG Advisory, Enterprise Risk Management in Italy, 2012.

regulations existing in different countries. This manual has been updated in 2009 and later in 2013.[27]

In 2004, the organisation presented the Framework *"COSO Enterprise Risk Management-Integrated Framework"*, which is not a substitute of the previous manual presented in 1992, because "internal control is an integral part of enterprise risk management, this enterprise risk management framework encompasses internal control, forming a more robust conceptualization and tool for management."[28] This framework has been proposed as a consequence of a clear importance recognised to risk management in relation with performance and, on the other side, as a response to the need of a system able to identify, evaluate and manage risk efficiently. The COSO framework has the objective of simplifying the fulfilment of business goals, boost performance and minimize losses, through the alignment with the risk management system.

A fundamental premise should be made: each organisation exists with the intent of creating value for its shareholders, this value is maximised when strategy and objectives are aligned to the risk management process, this guarantees a good balance between growth and risks connected to it. It is also important to remark the fact that ERM is a dynamic process, not a standardized process, which repeats itself; each ERM component can influence the others at any stage of the process. For these reasons ERM appears as an interactive and multidirectional process, which varies according to the company implementing it. It is difficult and incorrect to assume that ERM's characteristics remain always the same; each firm has its own risk management processes and needs according to the industry in which it operates, to its culture and the way in which the business is managed. Hence, the framework being discussed illustrates the model that firms should follow in order to implement a correct ERM approach; however the model can be adapted according to the characteristics of the company implementing it.

According to the framework, ERM:

- Allows to align risk appetite and business strategy: management should consider risk tolerance of the firm in order to evaluate the strategic alternatives, define targets and develop mechanisms to manage related risks;
- Enhances possible alternatives when it comes to manage risk;
- Supports losses minimizations and maximizes opportunities deriving from upside risk;
- Simplifies an efficient and integrated response to the variety of risks to which the firm

[27] www.coso.org

[28] Statement from the report *"Internal control-Integrated Framework"*, COSO, 1992.

is exposed;

- Improves resource allocation and evaluation of capital needs on the basis of information obtained.

According to the explanation provided by COSO framework (2004), ERM model is characterised by the existence of eight interrelated components: internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication, monitoring. We're going to describe briefly these eight components.

Internal environment – the internal environment encompasses the nature of the organization, and stand sat the basis of the view concerning risk, including risk management philosophy and risk appetite, integrity, ethical values and the environment in which they operate.

Objective Setting – objectives must exist before management can identify events potentially harmful for their achievement. ERM ensures that management planned a process to set targets and that chosen objectives support and align with the entity's mission, consistently with the risk appetite of the firm.

Event Identification – the firm must identify internal and external events affecting the achievement of its objectives, distinguishing between risks and opportunities. Opportunities should be sent back to the process of strategy setting or objective setting conducted by the management.

Risk Assessment – risks are analysed, considering likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and residual basis.

Risk Response – management selects risk responses (avoiding, accepting, reducing or sharing risk) developing a set of actions to align risks with the risk tolerance and risk appetite of the company.

Control Activities – policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.

Information and Communication – the company identifies, captures and communicates relevant information in a form and timeframe, which enables people to carry out their duties. Effective communication also occurs in a broader sense, following a top-down and bottom-up approach in the entity.

Monitoring – the whole of enterprise risk management should be monitored and

modifications are needed. Monitoring activity is accomplished through on-going management activities, separate evaluations or both of them.

These components, in order to be effective, have been related with the goals of the firm; ERM is a process implemented with the aim of meeting performance expectations and reaching goals. The framework categorizes the objectives into four groups.

Strategic objectives – high level-goals defined by the top management and aligned with the mission of the firm.

Operational objectives – targets related to the effective and efficient use of resources.

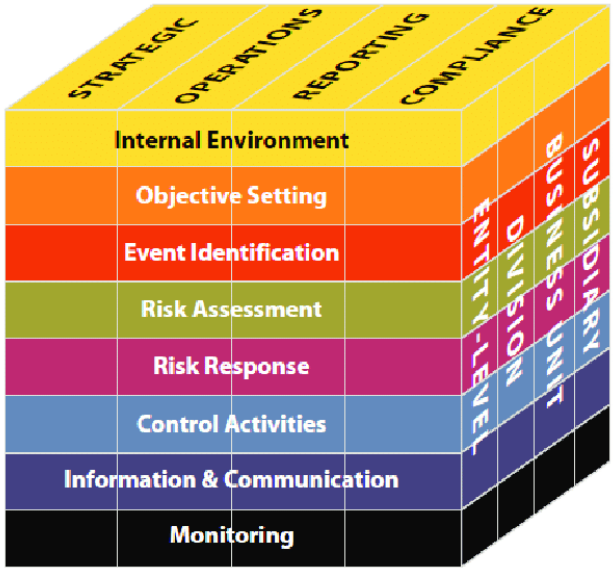
Reporting objectives – goals related to the completeness and reliability of information presented in the company's reports.

Compliance objectives – related to the compliance with applicable laws and regulations.

These categories described above shouldn't be considered as "separated boxes", they are all connected to each other, in fact in some cases one specific objective may fall under one or more categories. There is a strict relationship between the objectives set by the company (four groups of objectives) and the tools implemented to reach these objectives (eight components of ERM). For this reason the framework proposes a cube shaped matrix (Figure 1) to show the connection existing among ERM components and objectives, referring t the company as a whole but also to its business units.

The four objectives' categories – strategic, operations, reporting, and compliance – are reported on the vertical columns, the eight components on the horizontal rows, and the entity's units on the third dimension. This depiction portrays the ability to focus on the entirety of an entity's enterprise risk management, or by objectives category, component, entity unit or any subset thereof.

Figure 1-The cube Matrix representing the relationship between objectives and ERM components



Source: coso.org, ERM executive summary

Determining whether an entity's enterprise risk management is effective is a judgment resulting from an assessment of whether the eight components are present and functioning effectively. For the components to be present and functioning properly there can be no material weaknesses, and risk needs to have been brought within the entity's risk appetite. When enterprise risk management is determined to be effective in each of the four categories of objectives, respectively, the management has reasonable assurance that they understand the extent to which the entity's strategic and operations objectives are being achieved, that the entity's reporting is reliable and compliance with applicable laws and regulations is ensured.

As we have pointed out, the model proposed by COSO is considered quite flexible, due to the fact that it can be applied to the whole risk management process of the firm or to specific business units only. Even though the framework is very detailed and tries to provide a guideline in the implementation of an integrated management model, such framework has been highly criticised by literature and also in practice. The main limits can be summed up with: the focus of the framework places too much attention on the internal aspects of the company and the context in terms of internal and external factors is not specified; risks are presented only as events, without mentioning the uncertainty effect on objectives nor opportunities; risk management is described and explained only under the negative aspects of risk, without deepening the theoretical reference of the framework on the exploitation of

opportunities deriving from risks; there is no practical reference on how integration between ERM and strategic planning should be conducted.[29]

These limitations summed up to the poor consideration of the integration process, brought COSO to a complete revision of the ERM framework: the new document published in 2017 entitles "Enterprise Risk Management – Integrating with Strategy and Performance". The COSO itself stated that the Committee was pushed to produce a new framework because of a change in the complexity of risk and due to the emergence of new type of risks. Companies are interested in more detailed and improved risk reporting, so they see in the application of enterprise risk management process a great value. According to the Committee, the new framework provides greater insight into strategy and the role of ERM in strategy setting; furthermore it enhances the alignment between organizational performance and ERM, since risk management plays a fundamental role in terms of performance and impact on strategy. The new framework isn't characterised anymore by the eight components of the previous one, instead it consists of five interrelated components of enterprise risk management, which have a strong relationship with the entity's mission, vision and core values, and they affect performance; for this reason it becomes crucial to integrate enterprise risk management with strategy planning and day-to-day decision making.

The five components are:

- **Risk Governance and Culture**: risk governance and culture stand at the basis for all other components of ERM. Governance sets the tone of the company, with the aim of establishing responsibilities for the supervision of ERM and defining guidelines. Culture instead is concerned with the company's values, ethics and understanding of risk in the entity.
- **Risk, Strategy and Objective Setting**: the process of setting strategy and business goals allows the entity to integrate ERM into its strategic plan; by analysing the context in which the business operates, the organisation understands the impact to risk of internal and external factors and can set its risk appetite according to the strategy selected. The establishment of precise objectives in accordance with the strategy, allows to shape operations and priorities of the firm.
- **Risk in Execution**: an organisation tries to identify and assess risks that may affect the performance of the company and the ability to meet its goals, thus it prioritizes risks according to seriousness and the entity's appetite. The firm then monitors

[29] Dermot Williamson, *The COSO ERM framework: a critique from systems theory of management control*, International Journal of Risk Assessment and Management, Vol. 7(8), pp. 1089-1119, 2007.

performance; in this way it develops a "portfolio of risk" of the entity in the pursuit of its strategy and objectives.

- **Risk Information, Communication and Reporting**: management uses internal and external sources to gather relevant and quality information to support ERM. Communication is an iterative process of obtaining information and sharing it throughout the entity. All of the information gathered and processed through the information systems of the company becomes functional for reporting on risks, culture and performance.
- **Monitoring Enterprise Risk Management Performance**: through a periodical and constant monitoring of ERM performance, an entity can evaluate how well the ERM components are working and interacting between each other, also in the perspective of substantial changes.

These five components present within them a series of principles representing the fundamental concepts associated to each component (see Figure 2). These principles represent things that an organisation would do as part of its ERM practices and the management's job is to apply and judge them in a critical way.

Figure 2-ERM Principles

Source: coso.org, ERM framework, June 2016 edition

The framework proposed by the COSO provides a very detailed description of each principle contained in the five components. However, given the nature of the topic and the logical thread we want to follow in order to reach our final analysis, it is more interesting and functional for our itinerary to point out the key changes between the two frameworks from 2004 and 2017 proposed by the COSO, instead of analysing the peculiarities of the framework principle by principle. The new framework:

- Adopts a components and principles structure;
- Simplifies the definition of enterprise risk management;
- Emphasizes the relationship between risk and value;
- Renews the focus on the integration of enterprise risk management;
- Examines the role of culture;
- Elevates discussion of strategy;
- Enhances the alignment between performance and enterprise risk management;
- Links enterprise risk management into decision-making more explicitly;
- Delineates between enterprise risk management and internal control;
- Refines risk appetite and tolerance.[30]

In detail:

1) Adopts a components and principles structure

Similarly to the 2004 framework, the updated one presents a component structure with the addition of a series of principles, representing a fundamental concept associated with each one of the components.

2) Simplifies the definition of ERM

According to the feedback received by the COSO on its 2004 framework, it resulted that the definition of enterprise risk management was easy and clear for those in risk management roles, however its clarity wasn't so evident for people outside risk management functions. For this reason in the 2017 edition of the framework, the definition has been revised with the objective of improving clarity and memorability for everyone. The biggest news in the definition is the closer alignment between risk and value, noted as a key driver of enterprise risk management. *"The culture, capabilities, and practices, integrated with strategy-setting and*

[30] COSO, *Enterprise Risk Management Integrating with Strategy and Performance,* Frequently Asked Question Section, pp. 5-8, 2017.

its execution, that organizations rely on to manage risk in creating, preserving, and realizing value."[31]

3) Emphasizes the relationship between risk and value

As mentioned above, the revision of the definition of ERM emphasizes the role of enterprise risk management in creating, preserving and delivering value; ERM is not anymore focused only on preventing losses of value and minimizing risk, it rather deals with value creation and maintenance through integration with strategy setting and opportunities identification. This is the proof of ERM as a dynamic process, integrated with the managerial activity of the firm's operations.

4) Renews the focus on the integration of enterprise risk management

The new framework highlights throughout the whole document the importance of the integration of ERM with all the operations of the firm: starting with strategy setting, objectives setting and risk management. ERM's importance stands in the support provided not only to risk management, but also to organization's management in general, with the main goal of value generation and maintenance. COSO encourages users to consider ERM as an activity integrated with management, not an individual activity to be considered as a support.

5) Examines the role of culture

The first component presented in the framework embeds the concept of culture in its principles. Culture is represented as a fundamental element to influence the other components of the framework; understanding and shaping the culture allows the firm to determine the main path to follow in conducting its activities and determines the distinctive set of ethical values to be pursued during the operations.

6) Elevates discussion of strategy

A strategy that isn't aligned with the organisation's mission, vision and core values represents the main reason of failure. The new framework proposed in 2017 pones greater attention on the discussion of risk and strategy by focusing on the potential damages provoked by risk impacting strategy and remarking the importance of ERM in the identification, assessment and management of risks and its impacts on strategy.

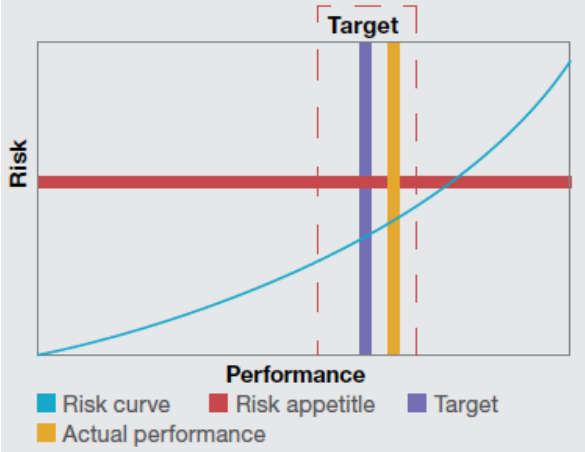
7) Enhances the alignment between performance and enterprise risk management

The framework, starting from the new title, underlines the centrality of risk in the decision of business objectives and targets; the document explores the importance of ERM in risk

[31] ERM definition provided by COSO, *"Enterprise Risk Management – Integrating with Strategy and Performance"*, June 2016 edition.

identification and assessment for what concerns impacts on performance, the determination of different profile risks according to changes in performance and emphasizes the importance of reporting in terms of impacts of risk on strategy and goals. The framework also proposes a new graphical representation of risk profile (Figure 3), which offers a dynamic and comprehensive view of risk, enabling more risk-awareness during decision-making processes.

Figure 3-Risk Profile



Source: coso.org, "Enterprise Risk Management – Integrating with Strategy and Performance", June 2016 edition.

8) Links enterprise risk management into decision-making explicitly

The document studies and explains how the information, such as type of risk and severity, potential influences on the business, entity's risk culture and appetite, gathered by the company on its risk profile enhances overall decision-making. Integrating ERM into the value chain and the lifecycle of an organisation supports and improves awareness of risk in decision-making.

9) Delineates between ERM and internal control

This new framework does not replace the one published in 2013 *"Internal Control-Integrated Framework",* instead it is complementary to it, in fact some aspects introduced in the 2013 framework, such as governance aspects of ERM, have been developed and more explicitly debated in the new document.

10) Refines risk appetite and tolerance

The new framework maintains the definition of risk appetite, however it refines the one of risk tolerance, which is explained using the language of performance and focusing on which is the amount of risk acceptable for a given level of performance.

The determination of the boundaries related to acceptable risk in the context of performance enables the firm to assess whether changes in performance remain within the limits of acceptable risk level. Risk and performance constantly influence and shape each other.

Also the cube matrix of the 2004 framework representing the relationship between the four categories of objectives and the eight components of the ERM process has been completely changed into a new graphical representation, with a helicoidal shape weaving the five components of the new ERM framework (see Figure 4). "The three strips ribbon represents the common processes flowing inside the organisation (strategy and objective setting, performance and revision), the two strip ribbon represents the ERM mechanisms supporting the other processes (governance and culture, information and communication and reporting)."[32]

It appears clear that the framework proposed and revised in its latest version by the COSO aims at promoting the importance of enterprise risk management as essential part of the strategic management, organisation's culture and as systematic process functional to the fulfilment of business objectives. The role of ERM doesn't consist only in an efficient and effective management of risks, but also in the integration of goal setting, risk management policy, definition of roles and responsibilities in strategic planning processes across all the value chain of the organisation.

Figure 4-Enterprise Risk Management

Source: Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Enterprise Risk Management – Integrating Strategy with Performance*, Executive Summary © 2017.

[32] D. Chesley, *The top changes to the COSO ERM Framework you need to know now* , Global, (APA) Risk Consulting Leader in PWC, 2017.

2.3 The role of Enterprise Risk Management in sustainable decision-making

In 2018, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and the World Business Council for Sustainable Development (WBCSD) released a guideline for applying enterprise risk management (ERM) to environmental, social and governance (ESG)-related risks. This guidance provides significant implications for integrating COSO's ERM framework into managing ESG-related risks. Given the significant increase in sustainability-related issues, it is important for companies to employ risk management as a tool to manage ESG-related risks and ensure business operational sustainability. This integration has a critical impact on an organization's sustainable development. Risk management is considered an important practice for improving sustainable decision-making. Unsustainable behaviours can generate potential business risks to an organization's reputation and ultimately result in the collapse of the organization itself. ESG-related risks arising from employees' unethical and unsustainable actions are preventable risks that are controllable and manageable through sound risk management. Implementing an integrated framework of ERM provides an essential foundation ensuring corporate commitments to ethical sustainability.

Over the last several decades, the prevalence of ESG-related risks has accelerated rapidly. In addition to a substantial rise in the number of environmental and social issues that entities now need to consider, the internal oversight, governance and culture for managing these risks also require greater focus. As a clear example of the growing importance of ESG related risks we can consider the evolution in the answers provided by businesses, governments, civil society and leaders to the surveys proposed by World Economic Forum's Global Risk Report: from 2008 to 2018 the risks rated as most dangerous in terms of impact and likelihood shifted from one societal risk, pandemics, to a series of environmental and societal risks, among which were included extreme weather events, water crises, natural disasters and failure of climate change mitigation.[33]

In the business world, this evolving landscape means ESG-related risks, that were once considered unlikely and improbable, are now far more common and can manifest more quickly and significantly. A report by the Society for Corporate Governance in the United States found that these issues often derive from a risk or impact related to the core operations and products of the company, can potentially damage in a significant way the company's

[33] World Economic Forum, *The Global Risks Report 2018, 13th Edition*, Retrieved from World Economic Forum: reports.weforum.org/global-risks-2018/, January 17, 2018.

value, reputation or ability to conduct its activities and are followed by persistent media interest, organized stakeholders and associated public policy debates that could magnify the impact of a company's existing position and increase the reputational risk created by a change in company policy or practice.[34] *"A company's ability to manage environmental, social and governance matters demonstrates the leadership and good governance that is so essential to sustainable growth, which is why we are increasingly integrating these issues into our investment process".*[35]

Nowadays entities are taking a more active role in addressing and understanding ESG-related risks, whether that means reducing or removing risk, preparing for risk and adapting to it or being more transparent about how the organization is addressing risk. Many entities have implemented ERM structures and processes to identify, assess, manage, monitor and communicate risks. Even in the absence of a formalized ERM structure or system, roles and responsibilities for risk management activities across the business are often defined and carried out. These processes provide a path for boards and management to boost performance and optimize outcomes, with the goal of enhancing capabilities to create, realize and preserve value. While there are many choices in how management can apply ERM practices, and no one better approach is universally better than another, research has shown that mature risk management can lead to higher financial performance. Exploiting these systems and processes can also support organizations in identifying, assessing and responding to ESG-related risks. Since ESG-related risks can be complex or unconventional for organizations to deal with, COSO and WBCSD, as mentioned previously, have developed a document to support entities to better understand and manage the full range of ESG-related risks.

The guidelines provided by this document are to be used by any entity facing ESG-related risks: including start-ups, non-profits, large corporations or government entities. The intended audience includes any decision-makers as well as risk management and sustainability practitioners who are looking for guidance on managing ESG-related risks. The audience may include those positioned in an ERM or sustainability function or with oversight responsibilities of those functions, but may also include any operations manager whose roles are impacted by ESG-related risks.

---

[34] Society for Corporate Governance and Brown Flynn, *ESG Roadmap: Observations and Practical Advice for Boards, Corporate Secretaries and Governance Professionals,* p. 6, June 2018.

[35] Fink, L., Larry Fink's Annual Letter to CEOs: A Sense of Purpose. Retrieved from BlackRock, 2018.

The purpose of this document is to help organizations apply ERM principles and practices to ESG-related risks; to this extent, the guidance applies the COSO's ERM Framework *Enterprise Risk Management—Integrating with Strategy and Performance*. While the guidance is aligned to the ERM framework's five components and 20 principles (shown in Figure 2 at par. 2.3), it also offers a practical approach, using other risk management frameworks, such as ISO 31000 or entity-specific risk management frameworks. Wherever possible, the document exploits existing frameworks, guidelines, practices and tools from both the risk management and sustainability fields. This guide is not intended to be used as an ERM guidance but should be used in conjunction with an established ERM framework. The main purposes of the guidance are the following:

Enhance resilience in organisations – the medium and long term feasibility and resilience of an organisation will depend on the ability to anticipate and react to a complex and interconnected series of risks that threaten the strategy and objectives of the business.

Offer entities a common language for articulating ESG-related risks - ERM identifies and assesses risks according to their potential impact on the strategy and objectives of the business. Articulating ESG-related risks in these terms brings sustainability issues into mainstream processes and evaluations.

Help organisations in improving resource deployment - obtaining robust information on ESG-related risks enables management to assess overall resources needs and helps optimizing resource allocation.

Enhance pursuit of ESG-related opportunities - by considering both upside and downside risks of ESG-related issues, management can identify ESG trends that lead to new opportunities.

Support organisations in realising efficiencies of scale - managing ESG-related risks centrally and simultaneously other business risks helps to eliminate redundancies and allows a better allocation of resources to address the entity's main risks.

Improve disclosure - improving management's understanding of ESG-related risks can provide the transparency in terms of disclosure that investors expect and support achieving compliance with reporting requirements.

Many of the governance issues, such as ownership, accounting and anti-competitive practices, have been long-standing issues for organizations, with which they had to deal since many years, and are generally well managed in strong and established ERM processes. The guidance therefore places greater attention on environmental and social issues, which for

some organizations have historically been managed outside the influence of governance and ERM. The governance risks discussed throughout the guidance tend to focus on either the governance of environmental or social issues, or other issues that have recently gained interest in the world of business, such as business ethics or diversity on boards.

The guidance is structured in five chapters reflecting the five components of the COSO ERM Framework published in 2017, starting with governance and culture, strategy and objective-setting, then moving through the ERM process focusing on performance (identifying, assessing and prioritizing and responding to ESG-related risks), review and revision and finally information, communication and reporting for ESG-related risks.

Governance and culture for ESG-related risks - governance, or internal oversight, determines the way in which decisions are made and how the company executes these decisions; applying ERM to ESG-related risks includes raising the board and executive management's awareness of ESG-related risks, supporting a culture of collaboration among those accountable for risk management of sustainability issues.

Strategy and objective setting for ESG-related risks - all entities have impacts and is dependent on the environment and society; therefore, a strong understanding of the business context, strategy and objectives is crucial for all ERM activities and the effective management of risks. Applying ERM to ESG-related risks includes examining the value creation process to understand how the organisation impacts and is influenced by the environment and the society in the short, medium and long term.

Performance for ESG-related risks

Identify Risk - organizations use multiple approaches for identifying ESG-related risks: megatrend analysis, SWOT analysis, impacts and dependency mapping, stakeholder engagement and ESG materiality assessments. These tools can help identify and express sustainability issues in terms of how a risk threatens the fulfilment of an entity's strategy or the achievement of business objectives. Applying these approaches through collaboration between risk management and sustainability practitioners elevates ESG-related risks to the risk inventory and positions them for appropriate assessment and response.

Assess and prioritize risk - companies have limited resources, so they cannot respond equally to all risks identified across the organisation. For this reason, it is necessary to assess risks in order for them to be prioritized. Applying ERM to ESG-related risks includes assessing risk severity in a way management can use to prioritize risks. Exploiting ESG subject-matter expertise is crucial to ensure that emerging risks or longer-term ones are not ignored or discounted, but instead assessed and prioritized appropriately.

Implement risk responses – the way in which an entity responds to identified risks will ultimately determine how effectively the entity preserves or creates value over the long term. Adopting a range of innovative and collaborative approaches that consider the source of a risk as well as the cost and benefits of each approach supports the successful outcome of these responses.

Review and Revision for ESG-related risks – this activity is critical for evaluating ERM's process effectiveness and modifying approaches if needed. Organizations can develop specific indicators to warn management of changes that need to be implemented in risk identification, assessment and response. This information is then reported to a range of internal and external stakeholders.

Information, communication and reporting for ESG-related risks - applying ERM to ESG-related risks includes discussing with risk owners, to identify the most appropriate information to be communicated and reported internally and externally, in order to support risk-informed decision-making.

The relationship between enterprise risk management process and the management of non-financial risks is a very current issue which challenges the world of business; being sustainable across all business activities ad managing risks connected to non-financial aspects may be considered the new frontier of risk management. The fact that in 2018 COSO and WBCSD worked jointly to provide a framework with some guidelines on how to integrate ERM activity with the management of non-financial risks is representative of the fact that ESG-related risks and aspects are gaining importance in the organisational landscape and stakeholders' concern on these issues and how the company deals with them is becoming more and more urgent.

Chapter 3

The relevance of non-financial risks and the impacts on performance

3.1 Identification and assessment process of Non-Financial Risk

Identifying a risk means individuating the sources of uncertainties, in other words those events implying impacts of different nature (economical or financial for example) on the company. The objective of the phase of identification consists in locating all risks potentially threatening the business activities of an organisation. During the process of risk management, identifying risks is a critical phase since there isn't any certainty in meeting the objective of identifying all risks through the different techniques available. As we have anticipated in the previous chapters, failing to identify even one single risk could be very dangerous for the firm and imply negative consequences such as poor performance or failure of a project; for this reason we stressed the fact that ERM activities must be carried out very carefully trying to follow the frameworks provided by international organisations, in order to enhance the chances of identifying and managing risks in the most effective way as possible.

Risks are present in all business activities; they often come into focus due to changes in business strategy, objectives, context or risk appetite.

Management can leverage the outcomes from these activities to gain a more complete understanding of their entity's risks. Generally, referring to risks in general (not only non-financial ones), there is no schematic process to be adopted for identifying risks: a general method consists in segmenting the organisation, the activities and the projects followed by the company and for each one of these try to identify all the negative factors that could potentially damage the operations of the company. This is a complex and costly procedure in terms of both time and money, however it allows to realize a complete map of business risks; furthermore, a correct risk mapping allows the company to evaluate risks more easily and identify those activities which need periodical managerial interventions.

As we have pointed out, there are no techniques guaranteeing the identification of all the possible risks faced by an organisation; thus the company is held to consider a series of fundamental aspects with the aim of maximising the efficiency of this phase of research and analysis. Companies should try to standardize the language inside the firm, in order to define and frame factors of risk at all levels of business, they should adopt more than one identification technique and the process should involve a team made up of members from

different functions of the organisation in order to bring up all the issues pervading the company.

The identification process for non-financial risks that impact performance or strategy in a company turns out to be more complex to carry out. Not all factors, especially if we consider risks related to environmental, social and governance issues, present an enterprise-risk level, which means that managers' ability stands in translating external trends and factors into identified risks, in order for them to assess eventual consequences on the organization. Certainly, many entities produced methods and processes to manage these types of risks, however there are a series of factors, which make ESG risks more challenging than other non-financial risks[36]:

- Often they are emerging kind of risks that could threaten organization performance in unexpected ways;
- In some cases these risks represent "black swans"[37], so they become unpredictable and very challenging to manage;
- ESG risks are long-term risks, which can go beyond the plans of the company, including strategy or risk evaluation;
- These risks are difficult to quantify and communicate in the business context;
- Generally, ESG risks go beyond the scope and purpose of the single entity, therefore they should require responses at industry or government levels.

According to the COSO ERM Framework*, the objective of risk identification is to determine the risks that could interrupt operations affect the reasonable expectation of achieving the entity's strategy and business objectives or materially impact the entity's license to operate (including reputational issues)[38]*. Identifying opportunities should be a key part of the risk identification process; COSO defines opportunities *as the actions or potential actions that create or alter goals or approaches for creating, preserving and realizing value[39]*. Many entities maintain a risk inventory or register to list the risks they face. This inventory provides common categories and standard definitions through which risks can be described and discussed. A risk inventory may also include a brief description of the impact of each risk, mitigation actions and the risk owner. If we take under analysis ESG-related risks: when these threats

[36] COSO and WBCSD, *Enterprise Risk Management-Applying enterprise risk management to environmental, social and governance-related risks,* pp.40-41, October 2018.

[37] The black swan theory was developed by Nassim Nicholas Taleb, who describes it as "first, it is an outlier, as it lies outside the realm of regular expectations, because nothing in the past can convincingly point to its possibility. Second, it carries an extreme impact. Third, in spite of its outlier status, human nature makes us concoct explanations for its occurrence after the fact, making it explainable and predictable."

[38] COSO, "*Enterprise Risk Management: Integrating with Strategy and Performance",* p. 67, June 2017.

[39] Ibidem

meet the entity's risk criteria, they should be included in the risk inventory, in order for them to be managed and monitored. Typical categorization of risks in risk inventories include strategic, operational, financial and compliance. Some organizations may include a separate category for "sustainability" or "reputational" risks, however these risks can usually be grouped in other categories (for example, climate-related risks are often operational or financial in nature). Furthermore, reputational implications are often a consequence from another type of risk, rather than a risk of itself (for example, reputational damage of the image of an organisation resulting from an environmental incident or pollution). In addition, many non-financial risks are not entirely new but rather represent an additional source to an existing risk or compound the risk's impact or likelihood of materializing. For example, climate change impacts often increase the risk of raw materials cost fluctuations, which is an existing risk for many entities.

Many entities implement an ERM process to identify risks that impact the business strategy and include them in the risk inventory. This process may include surveys, workshops and interviews with risk owners and executives to confirm existing risks or understand new or emerging risks. In addition, entities have on going activities and processes performed by the sustainability function, corporate strategy function or risk owners that can support the identification of ESG-related risks. Some of the approaches used to identify non-financial risks include:

Data tracking and analysis of past events or issues – this type of analysis is fundamental for identifying the principal risks threatening the business; it can be based both on personal experience from members of the company or on documents containing information on business related risks. The main limitation of this type of analysis is the lack of documentation sufficiently exhaustive, in order to provide a consistent base for risk management, in fact the attention for an integrated vision of risk management (especially for non-financial risks) is quite recent and, in any case, analysis of past events allows you to look only in the past, without giving the chance to focus and prepare for upcoming events; in this way companies tend to overestimate existing risks and underestimate unknown or potential issues impacting the activities of the business.

Internal audit and surveys – interviews and internal research permit to overcome the limitations of data analysis, in fact providing surveys or interviewing subjects inside the organisation allow a more efficient identification of non-financial risks pervading the company. This method is particularly useful since it allows to gain information from people pertaining to different units and functions of the business, so it gives the management the

possibility to understand all the issues to which the company is exposed, even those with a more technical nature, which otherwise wouldn't be recognised.

SWOT analysis - a SWOT analysis uses a two-by-two matrix to define the strengths, weaknesses, opportunities and threats an entity is facing. This type of analysis considers both internal and external factors, so it is commonly used by organizations as a strategic planning tool. The World Resources Institute (WRI) has developed a sustainability-specific SWOT tool focused on understanding the SWOT from an ESG perspective (i.e., impacts, dependencies and related megatrends) designed to help drive action and collaboration on environmental challenges creating real business risks and opportunities. It helps individuals engage and motivate colleagues, particularly those with limited knowledge of environmental issues or corporate sustainability.[40]

Stakeholder Engagement - different stakeholders may have different perceptions of value and different expectations of an entity's roles and obligations. Within sustainability, the concept of stakeholder engagement refers to the process used by an organization to engage relevant stakeholders for the purpose of achieving shared outcomes. The process can be used to help all parties better understand the business context, including issues or risks that may otherwise be underestimated by risk management practitioners, sustainability practitioners and the business in general. It provides outside perspectives of events and enables entities to question and challenge assumptions, to confirm existing risks and identify new or emerging risks.

When identifying risks, it is important to go beyond a simple "list"; rather, risks should be articulated precisely in terms of the impact on the strategy and business objectives as well as understanding the nature and original source of the risk. Not all non-financial issues identified by an entity's materiality assessment or analysis should be included in the risk inventory. For some risks, it may be appropriate for sustainability practitioners to perform on going monitoring and evaluation, to verify whether these risks should be elevated to an enterprise level and included in the risk inventory in the future. Regardless of whether the risk is included in the enterprise risk inventory, once a risk has been identified, risk management and sustainability practitioners can deploy ERM processes outlined in the previous chapter to assess, prioritize and react to the risk taken under consideration.

---

[40] Metzger, E., Putt del Pino, S., Prowitt, S., Goodward, J., Perera, A., *SWOT: A Sustainability SWOT.* Retrieved from World Resources Institute: http://pdf.wri.org/sustainability_swot_user_guide.pdf.

When identifying risks, practitioners should aim at precisely describing each risk. The description should focus on the risk itself, rather than calling out a general ESG or other non-financial issues, the root cause of the risk, the potential impacts of the risk or the effect of the risk response being poorly implemented. In accordance with COSO, accurate risk identification enables the organization to: effectively manage the risk inventory and understand its relationship with the business strategy, objectives and performance, accurately assess the severity of a risk according to the business objectives, reduce the "framing bias" that can occur when a risk is framed to focus on either the potential upside or downside effects.

Effective risk management requires constant balancing of risk exposures, benefits and expenditures. For this reason, management assesses the severity of risks to support prioritization and maximize the strategic, financial and operational benefits for the entity. Non-financial risks can be challenging to assess and prioritize: by nature, the financial or business implications of non-financial issues may not be immediately clear or measurable. These challenges are often worsen by an organization's limited knowledge of non-financial risks, tendency to focus on short-term risks without paying enough attention to risks that may arise in the longer term or difficulties in quantifying less conventional risks. Even when the severity of a non-financial risk can be quantified, the outcome may still be uncertain. Finally, the risk of not prioritizing appropriately a non-financial risk could simply be due to a unconscious bias towards risks that are well known or more intuitive. The assessment and prioritization of non- financial risks follows the same processes put into effect for financial and more conventional risks, which companies are more used to manage. However, as anticipated above, verifying and quantifying the severity of non-financial risks and prioritizing them is a challenging procedure. For this reason, instead of focusing on the ways in which risks are assessed and prioritized, for the sake of the topic treated by this paper, the focus is going to shift towards the kind of challenges caused by non-financial risks (especially ESG-related ones) in the assessment phase. To this end, COSO ERM framework tries to provide some guidelines in defining the impact and the likelihood of a specific event as part of the risk assessment process conducted by managers. Even though these two criteria are common criteria for prioritization, sometimes they can lead to poor assessment and wrong prioritization. In fact, PwC published a document outlining some of the characteristics of non-financial risks (especially ESG factors) that make them different from more traditional risks and cause some challenges in the assessment phase. ESG-related risks can be more unpredictable and manifest over a longer and often uncertain time frame. Assessment of risk

is often based on historical data and for ESG-related risks, particularly those that are new or emerging, it can be difficult to find historical information to estimate the risk impact. ESG-related risks are macro, multi-faceted and interconnected and can affect the business on many dimensions; this can make assessing an ESG-related risk more complex. Risks may be outside an entity's control, so reacting to it may rely on the actions of other parties or may require coordinated efforts.[41]

ESG-related risks also tend to be affected by organizational biases that exist during assessment and prioritization. Specifically, organizational bias can lead to a failure in identifying the full range of outcomes that may derive from a risk, or overconfidence in the accuracy of risk assessments and mitigations procedures in place. There is also a tendency for individuals to link risk assessment estimations based on readily available evidence, despite the limitations of using recent historical data to an uncertain and variable future. This bias is often compounded by confirmation bias, which drives individuals to favour and consider valid information that supports a certain idea and reject information that contradicts that position.

To help organisations overcome these challenges, COSO proposes a list of additional that could provide a more complete understanding of the nature of non-financial risks and the level of exposure of the company. This list can be used for assessing and prioritizing risks for non-financial risks in order for the company to order them according to relevance.[42]

The criteria proposed by COSO are the following:

Adaptability – which is the capacity of an entity to adapt and respond to risk

Complexity – the scope and nature of a risk to the entity's success

Speed of onset – the speed at which risk impacts an entity

Persistence – for how much time a risk impacts an entity

Recovery – the ability of an entity to return to tolerance

The risk exposure of an organisation is not a static situation: the company is an entity evolving across time; hence the phase of risk assessment can't be carried out sporadically, it has to be a constant and periodical activity. Furthermore, a minimum level of risk assessment frequency should be ensured, with the objective of integrating risk management with the normal functioning of the company, trying to align it with strategy setting and objective setting, avoiding the unproductive situation of a simple exercise of compliance.

---

[41] Borsa L., Frank, P., Doran, H., *"How can resilience prepare companies for environmental and social change?"*, Resilience: a journal of strategy and risk, Retrieved from PwC: https://www.pwc.com/gx/en/governance-risk-compliance-consulting-services/resilience/publications/pdfs/resilience-social.pdf.,

[42] COSO, *Enterprise Risk Management: Integrating with Strategy and Performance,* p. 79, June 2017.

3.2 The effects of non-financial risks on performance

Integrating non-financial policies and practices into a company's strategy and daily operations is considered by investors as relevant in order for the company to realise long-term value. Therefore, transparency around how a company manages non-financial risks and opportunities is part of its value proposition. As a result, the financial community increasingly recognises that to thoroughly assess an investment, it must also analyse relevant non-financial factors, such as ESG ones for example. While ESG factors are at times called non-financial, how a company manages them undoubtedly has financial consequences on the performance of the business, on the evaluation of investors and stakeholders in general.

In the last decade companies continued to investigate whether paying attention to non-financial issues and, as a consequence, to risks deriving from these factors actually enhances mitigation of these risks and performance in general. In other words, organisations have been investigating whether being sustainable, so pursuing a growth strategy through allocation of resources on non-financial practices and issues, actually gives the company the possibility to exploit new opportunities in favour of a better performance.

According to a review of empirical research conducted by Matteo Tonello and Thomas Singer (both part of the Conference Board Inc.), regarding the returns in terms of performance from implementing non-financial practices, there are five main benefits deriving from investments in non-financial risks management[43]:

- Enhance market and accounting performance

Multiple empirical studies conducted in the last decade show that companies adhering to strong non-financial standards enjoy high profits, low capital expenditures, and high stock return. A study conducted by Harvard Business School[44] based on the observation of a sample of 180 companies demonstrated that those ones, which voluntarily adhered to a series of ESG practices, outperformed in the long term the other set of companies. The authors theorised that the reasons of such outperformance stand in the explicit assignment to a board of the sustainable risks management, or the propensity to engage with stakeholders and disclose non-financial information to the market. Another study[45], positioned earlier in time, argued that customer satisfaction mediates the relationship between ESG factors and

[43] Singer T. and Tonello M., *The Business Case for Corporate Investments in ESG Practices,* The Conference Board Inc., July 2015.

[44] Robert G. Eccles, Ioannis Ioannou, and George Serafeim, *The Impact of Corporate Sustainability on Organizational Processes and Performance*, Management Science 60, no. 11, pp. 2835-2857, November 2014.

[45] Xueming Luo and C.B. Bhattacharya, *Corporate Social Responsibility, Customer Satisfaction, and Market Value*, Journal of Marketing 70, no. 4, pp. 1-18, 2006.

performance given an increase in the sensibility towards these factors in the consumer market; in fact the correlation is more evident in the business-to-consumer industry.

- Lower the cost of capital

It is shown that publicly traded firms may reduce their cost of capital by adopting strong ESG practices. This relationship has been studied more in depth in terms of corporate governance practices; in fact most of the analyses attribute this finding to the mitigation of business risks resulting from the adoption of superior governance practices. From a less recent study published in 2007 it results that "*lenders believe that better-governed companies are subject to fewer cases of shareholder suits or government investigations, and that they are less exposed to disruptions by activist investors".*[46] A more recent article published in 2011 states that firms publicly exposed to environmental and social concerns faced shorter maturities and higher loan spreads and that socially responsible companies, which tended to voluntarily disclose this information, led to more accurate coverage by analysts and better company valuations.

- Engage with key shareholders

Corporate investments in non-financial factors may help to attract to the company's shareholders class a whole category of long-term investors that is increasingly gaining influence; it also offers new opportunities for companies to engage with large institutional investors sensitive to these emerging issues. Supporting this theory is the fact that the volume of proposals on social and environmental policy issues rose to unprecedented levels in 2014 according to The Conference Board dataset.

- Improve business reputation

If investments in management of non-financial aspects do not satisfy immediately operational and financial needs, they can be strategic and long-term, since they enhance relations with key stakeholders (employees, customers, suppliers, or local communities where the company operates). Over time, the perception of the brand benefits from these improved relationships: talent recruitment and retention, customer satisfaction, and the quality of media coverage are areas of intangible business success where the effects of an effective management of non-financial issues, a good mitigation of connected risks and a wise exploitation of opportunities can be easily monitored. Research published in 2014 by The Conference Board in collaboration with CSRHub explored the link between sustainability performance and Brand Finance's Brand Strength Index (BSI), a proprietary methodology to calculate the brand value

[46] Lucian A. Bebchuk, Martijn Cremers, and Urs Peyer, *CEO Centrality*, NBER Working Paper no. w13701, December 2007.

of more than five thousand leading global companies. The study revealed that about 22 per cent of the variation in BSI was explained by changes in perceived ESG performance.[47] "*Corporate reputation and sustainability are therefore related, and a company that seeks to do well in one area should also consider investing in the other."*[48]

- Foster revenue growth through product innovation

An increasing number of companies recognize that non-financial initiatives, especially those ones related to ESG issues, can yield new market opportunities, stimulate innovation in products and services, and ultimately be an important source of revenue. In fact, researches conducted by The Conference Board in 2015 examine the extent to which a sample of S&P Global 100 companies generates revenue from sustainability initiatives.[49] There are several examples of companies that have developed successful products or new lines of business built on sustainability considerations The development of these products can be motivated by a variety of factors: cost savings and efficiencies (for example using fewer materials), customer demand (longer-lasting products, products free of hazardous materials), or regulatory developments (products with lower GHG emissions). In many cases these products represent a rapidly growing source of revenue and an increasingly larger share of companies' total revenue.

More specifically, for what concerns non-financial risks and their effects on performance, a study conducted by Moneva J. and Cuellar B.[50] contributes to the environmental literature by exploring the effects and value relevance of non-financial information reported by companies in their annual reports. In their research an initial literature review shows how stock markets, at first, negatively assess the information offered by the companies most affected by the standards, anticipating the economic effects of their implementation; however, once the technological investments have been consolidated and the information disclosed reflects lower environmental risks, the market value increases.

According to Thomas Kaiser (2015)[51], non-financial risks require appropriate identification, management and controlling, because a mismanagement or undervaluation of these types of

[47] Bahar Gidwani, *The link between Sustainability and Brand Value*, in Thomas Singer (Ed.), Sustainability Matters, Research Report, R-1538-14-RR, p. 25, 2014.
[48] Singer T. and Tonello M., *The Business Case for Corporate Investments in ESG Practices,* The Conference Board Inc., July 2015.
[49] Thomas Singer, *Driving Revenue Growth Through Sustainable Products and Services*, Research Report No. R-1583-KBI, The Conference Board, June 2015.
[50] Moneva J and Cuellar B., *The Value Relevance of Financial and Non-Financial Environmental Reporting,* Environment Resource Economics 44, pp. 441–456, 2009.
[51] Kaiser T., *Managing non-financial risks: A new focus area for executive and non-executive board members*, Journal of risk management in financial institutions, 2015.

risks can exhibit their consequences after several years in the long-term and allocating impacts to individual events in a clear way becomes almost an impossible task. Non-financial risks are often strictly related among each other and the effects of one risk generally reflect on another one, and so on. For example, mitigation of environmental risks represent a big challenge for most business in general; if companies aren't able to implement affective plans to control their environmental impacts, then reputational risks arises due to a bad message sent from the company, which assists to a brand deterioration and as a consequence also business performance gets negatively influence. The author also claims that non-financial risks, due to the fact that they are mostly based on qualitative information and individual judgement, represent on one hand an opportunity for the company to communicate to investors their engagement in ESG activities and on the other hand non-financial risk disclosure, when excessively positive in the tone, may arouse suspicion in investors and the consequences can be very harmful in terms of a fall in the stock market or a decrease in brand reputation.

Non-financial risks represent the latest frontier of risks faced by companies and their management is an activity, which results costly in term of time, financial resources and human capital. Given the fluidity of the topic and the multi-sided impact that it has on the various business activities, the collaboration of both a top-down and bottom-up approach is needed in order to mitigate these types of risks. For this reason, non-financial risk management results very expensive in the short term, however results start to emerge only in the long-term so it is necessary, from the managerial perspective, a constant and consistent implementation of identification and mitigation activities to actually experience the benefits of an efficient non-financial risk management system. Avoiding or limiting the management activities of non-financial risks or focusing only on specific risks to save resources is going to damage the company in the long run, in terms of reputation, profitability and assessment by investors (rating).

Organisations have been investing in non-financial practices more frequently in the last decade. However, these resource allocations often respond to immediate business needs rather than a strategic and cohesive sustainability program intended to enhance the long-term key intangible assets in the environmental, social, and governance spheres. While empirical research on the link between corporate investment in non-financial factors and firm performance is still very active and controversial, several studies led by different institutions have shown that a company can be rewarded for adopting these practices with higher profits and stock return, a lower cost of capital, and better corporate reputation scores. To this

intention, it should be highlighted the fact that most controversies and debates concerning the impacts of non-financial issues on performance derive from the fact that most studies do not distinguish between material and immaterial sustainability issues. A paper published by three professors from Harvard Business School point out that "*investments in material sustainability issues can be value-enhancing for shareholders while investments in immaterial sustainability issues have little positive or negative, if any, value implications".*[52]

[52] Khan, Mozaffar N., George Serafeim, and Aaron Yoon. *Corporate Sustainability: First Evidence on Materiality*, Harvard Business School Working Paper, No. 15-073, p.20, March 2015.

3.3 Need of a holistic approach to Non-Financial Risk management

The political and social context influencing the activities of the company, have always affected the decisions and the behaviours of these ones over time. Until a certain time in history, society required business activities to aim at maximizing the economic value generated, in order to increase returns for shareholders. However, during time, the idea of economy experienced an evolution and as a consequence, requests and expectations towards organisations started to grow. As a matter of fact, when issues related to environmental situations and society started to assume greater importance, the whole civil society and the world of business started to observe and discipline attitudes and responsibilities of the companies on these topics. In particular way, not only shareholders and investors continued to demand maximum profits, but also a wider and relatively new group of stakeholders started to show interests and expectations concerning the new social and environmental issues. For these reasons, organisations decided to satisfy these requests and enhance the efficiency of their relational management attitudes towards stakeholders; companies begun to disclose more and more information concerning not only the main financial results of the company, but also responsibilities, behaviours, beliefs and values, in order to satisfy the new set of interests arisen among stakeholders. Due to this desire of going beyond the financial aspects and the interest in learning more about the reality of an organisation, corporate reporting grew and expanded its radius of action, adding to financial disclosure information of a different nature, but absolutely connected to its results and outcomes.

Non-financial reporting represents a wide range of topics for which organisations are accountable; the more the value of the company is connected to stakeholders and resources provided by them, the more accountable the company is for this issues and the more information is going to be disclosed.[53]

Non-financial reporting emerged when society started to perceive the idea of accountability from organisations. The first forms of non-financial reporting arose in the nineteenth century, with the birth of issues such as women rights and equality between workers during the Industrial revolution.[54] From this period onwards corporations started to disclose first social reports; later in time the attention started to move towards environmental issues, especially in the 90's, when the OECD published in 1991 a first group of environmental indicators (*Environmental Indicators: a preliminary set*). However, the true evolution, which started off

[53] Mitchell R. K., Van Buren H. J., Greenwood M., Freeman, R. E., Stakeholder Inclusion and Accounting for Stakeholders, Journal of Management Studies, Vol. 52 Issue7, pp. 851–877, 2015.
[54] Carroll A.B., Buchholtz A. K., Business & Society: Ethics, Sustainability, and Stakeholder Management, 8th edition. Cincinnati, OH: South-Western Cengage Learning, 2012.

the development, took place in 1992 with the UN Earth Summit in Rio de Janeiro[55], during which society was sensitized on environmental topics; due to this the request and disclosure of non-financial information grew exponentially. A further renovation took place after the Summit on Sustainable Development of Johannesburg in 2002[56] during which the idea of accountability by organisations led companies to embrace both social and environmental issues in its reports, which started to be called "sustainable development reports". In more recent years instead, the need to group all issues of social and environmental issues brought to the idea of "non-financial" subject, which finds its expression in an European directive issued in 2014, with the objective of regulating this type of disclosure, however this is a topic which is going to be discussed in the next chapter.

This brief description on the history of non-financial information leads to the understanding of the centrality of non-financial aspects in the conduction of business activities, especially if we take under consideration the risks emerging from this issues. For this reason a global approach to non-financial risk management is necessary, to ensure a correct evaluation of non-financial situations and the risks linked to them.

In recent years, the media have reported increasingly high losses incurred by the organisations and financial institutions, which have also had a negative impact on their reputation. Institutions cannot allocate these losses to the traditional financial risks (such as credit, market price or liquidity risks); instead, they fall into the risk category of non-financial risks (NFR). As mentioned above, NFR also comprise risks explicitly excluded from the supervisory definition of operational risks, such as strategic or reputational risk.

The wide range of non-financial risks causes complexity in the management activity of those risks that can currently be observed on the market, as well as the challenging moments of identifying, assessing, managing and reporting consistently and without redundancy in a non-financial risk framework. Very often, organisations face a series of challenges in managing non-financial risks and reporting on them; some of these tasks can be summarized in the following aspects:

- The responsibility and difficulty for non-financial risk management team to organize and report information for a big variety of stakeholders with different interests and focuses.
- Identify methodologies and metrics to identify and assess non-financial risks.

[55] http://www.unesco.org/education/pdf/RIO_E.PDF
[56] http://www.un-documents.net/aconf199-20.pdf

- Non-financial risk management has an ambiguous and eclectic role due to the variety of issues it has to deal with.

A consistent response to the challenges described above is necessary in order to establish effective non-financial management within the organisation, which meets the requirements of consistent reporting to stakeholders.

In practice, there is often no stringent analysis and derivation of strengths and weaknesses as well as opportunities and risks from the business model or business strategy. This increases the danger that opportunities and risks are not identified or are identified too late. The inclusion of the business model is essential in NFR management. Only with a deep understanding and inclusion of the business model and an analysis of the company's strengths and weaknesses is it possible to define a suitable business strategy and appropriate risk strategy including risk appetite, ultimately to be able to derive and manage new non-financial risks effectively. In addition, non-financial risks are often questioned and managed separately according to the different disciplines within the company (such as compliance, business continuity management, IT security, environmental regulations, etc.). Due to these section divisions, the identification and assessment of risks and controls in the departments often takes place inconsistently or inadequately. Silo assessments and inconsistent methods lead to additional effort and lack of understanding in the departments and ultimately to an insufficiently lived risk culture (as it has already been pointed out and analysed in the previous chapters, discussing the benefit of an integrated vision of risk management when running an organisation, see Chapter 2). In addition, the management usually does not yet receive a targeted and integrated report on non-financial risks. Due to the prevailing silos and uncoordinated management, reporting is also not targeted and coordinated.

An integrated and holistic view of non-financial risks should start with the continuous review of the business model and business strategy, taking into account current trends, internal and external conditions and factors. Current circumstances, such as the implementation of digital technologies, open up opportunities but also risks. In order to optimize the opportunities to exploit the positive side of risks, it is crucial to determine the risk-bearing capacity and risk appetite within the framework of a suitable risk strategy. Both opportunities and risks must be made transparent and consciously managed in accordance with the risk strategy and risk appetite of the organisation. Risks should be evaluated both quantitatively and qualitatively according to their various effects and actively reduced through the targeted use of appropriate controls. Actively mitigating risks helps to reduce capital requirements and also

reduces the probability of reputational damage or fines due to potential compliance incidents (see paragraph 3.2).

Common and uniform output parameters (such as IT systems) as well as consistent identification and assessment methods regarding risks and controls across different disciplines in the company represent a prerequisite for an integrated and holistic approach. Regular defence assessments in the form of risk and control assessments should be conducted at all levels of the enterprise; the management of the assessments should be centralized and coordinated by the board in coordination with other relevant central functions. The assessment process ultimately results in a targeted and integrated reporting system to the management; the report should contain the results of the assessments and thus provide the management with information relevant for conducting controlling activities.

The optimization potential with regard the non-financial risk management framework varies from company to company and should therefore always be examined individually. Optimization potential can be identified and designed specifically in the context of a preliminary study. A key phase in an hypothetic framework for NFR management should be the evaluation of the existing strategies, processes, methods, assessments, and systems in the company in order to derive synergies and optimization potential. The preliminary study goes one step further and ultimately has the goal of presenting company-specific alternatives and developing a desired solution.

Components of a non-financial risk framework should include a clear definition and delineation of which risks are considered non-financial, the establishment of methods for managing non-financial risks, and responsibilities with the aim of speaking a “common language”. This would provide an overall profile that could be reported consistently, while identifying synergies between non-financial risks, and lowering costs. In the long term, proactive management of these types of risks could also benefit the organisation; in fact it should be recalled the concept that non-financial risk management is part of that processes and business culture which is represented by ERM. As we mentioned in the previous chapters, the view of an ERM approach is embedded in the idea of a proactive system, which tries to anticipate the effects of risks on the activities, mitigating the negative ones and exploiting the opportunities represented by the potentially positive consequences.

Chapter 4

Risk Disclosure: enhancing the involvement of stakeholders

4.1 The evolution of reporting: from financial to integrated reporting

Accounting has been defined as the language of business, more specifically as Language for Specific Purposes (LSP) in order to show that its application is addressed only to specific social groups with a specific objective. Financial reporting, in its oldest and most traditional acceptation, is associated to the revision and reporting activity of financial statements, which is a discipline governed by strict regulations and norms. Over time, such discipline started to expand accordingly with the discipline of business economics and started to include more information concerning general corporate information, operating highlight, management's analysis and narrative texts. These reports, which obviously increase their complexity and add new terms for the evaluation of companies, take the name of annual reports.

Annual reports could be defined as formal financial statements that are published each year and disclosed to shareholders and other interested parties of the company; as it has been pointed out, these reports provide not only financial information, but also highlight the achievements of the company in the past year, promote the company through descriptions of its mission, vision and history and more in general discuss the operations of the company and upcoming prospects for the future. These annual reports have double value relevance: for sure the aspects discussed in the reports are going to interest internal parties such as the management and individuals involved in daily operations of the firm, but also stakeholders external to the company will be interested in the results and in the prospects of the company, for example potential investors are going to evaluate the performance of an organisation and according to the information included in the report could decide whether investing is a good deal or not.

Even though annual reports represent a step forward with respect to pure financial reporting, it is still not sufficient as a reporting tool, because it is unable to follow the evolution of business world and society, which has been rapidly changing in the last decades. In fact, there are several limitations connected to the adoption of an annual report:

- This type of reporting is unable to keep up with the evolution of the economic context, since it is excessively focused on mainly financial aspects involving the reality of an entity.
- Annual reports are backward oriented, which means that they contain information pertaining to the past, so it's usefulness turns out to be limited for stakeholders in the prediction of future results and in the evaluation of long-term performance.
- Annual reports lack completely of non-financial information concerning social, environmental, governance, operational and human aspects.

Hence, this series of limitations result in a general decrease in reliability and truthful report of information for annual reports; practitioners and stakeholders aren't confident anymore in the usefulness and fair representation of companies proposed by annual reports, there is the necessity of a new form of disclosure integrating more aspects and issues involved in the activities of an organisation.

Actually, the will of the world of business and society pushes reporting towards a new frontier in the contents of reporting: non-financial information.

Empirical studies on sustainability originate in the 70s with the seminal survey conducted by Ernst and Ernst in 1977 on a sample of 500 USA companies and are based on understanding accounting as a social phenomenon.[57] These studied continued in the following years in other Anglo-Saxon countries such as UK, New Zealand or Australia and the results were similar: the provision of non-financial information verified mainly with a higher prevalence in the USA, the UK, New Zealand, and Australia, an isolated phenomenon and not a systematic activity. Most of the non-financial information disclosed concerned human resources and community involvement issues, with minor references to environmental issues; only in certain critical industry sectors belonging to primary and secondary industries, such as mining, oil and steel companies, environmental disclosure obtained greater diffusion. Another common outcome of past researches include the prevalence of a qualitative rather than a quantitative disclosure: the tendency to emphasize only the good news by disclosing the information in a "self-praising" way and the positive association between the extent of non-financial disclosure and the firm's size.[58]

The term "non-financial" has been given different definitions and interpretations; for the sake of this thesis, we're going to interpret this term associating it to the wide context of

[57] Guthrie J., Parker L.D., *Corporate social reporting: A rebuttal of legitimacy theory.* Account. Bus. Res., 19, pp. 343–352, 1989.
[58] Deegan C., Gordon B., *A study of the environmental disclosure practices of Australian corporations*, Account. Bus. Res., 26, pp. 187–199, 1996.

sustainability, which has been defined in the report "Our common future" published by the World Commission on Environment and Development (WCED) as *"the development which meets the needs of current generations without compromising the ability of future generations to meet their own needs"* [59]. This report promoted sustainability as a means of balancing economic and environmental issues and encouraged organisations to aim at a sustainable development.

In response to the increasing pressures coming from national and international regulations, and society in general, corporation are gradually pushed towards the adoption of principles of both social and environmental responsibility within their strategies, structures and management systems. The growing need for an integrated approach towards sustainability at a systemic level inspired different organisations to work towards the provision of some guidelines or practices which could effectively support companies in carrying out this "mission" of being more sustainable in their activities and, as a consequence, in the reports disclosed. According to Nolan (2007), this extended reporting *model "aims to highlight the view that a company's consideration of only financial matters as an indicator of its success is inadequate."*[60]

Among the different organisations who worked, and are still working, on the topic of sustainability the one which is more active in this landscape is the Global Reporting Initiative (GRI)[61], founded in Boston in 1997. In concrete, GRI's efforts consisted in providing guidelines offering an international relevance for all companies interested in the disclosure of governance approach and of the environmental, social and economic performance and impacts of their activities. The framework prepared by the GRI has been first published in 2000 (G1 framework), and then revised in the following years until the last document, expanded and improved, has been released in 2013 (G4 framework). In 2016, GRI transitioned from providing guidelines to setting the first global standards for sustainability reporting – the GRI Standards. The Standards continue to be updated, including new Topic Standards on Tax (2019) and Waste (2020). The reason moving this organization to provide such guidelines stands in the lack of international directives, explaining or providing preliminary frameworks on how organizations should report non-financial issues and which

[59] United Nations, Report of the World Commission on Environment and Development, *Our Common Future*, New York: Oxford University Press, 1987.

[60] Nolan J., *Corporate Accountability and Triple Bottom Line Reporting: Determining the Material Issues for Disclosure,* In Enhancing Corporate Accountability: Prospects and Challenges Conference Proceedings; University of New South Wales: Kensington, Australia, 2007.

[61] 78% of reporting companies worldwide refer to the GRI reporting guidelines in their CR report, according to KPMG, *The KPMG Survey of Corporate Responsibility Reporting*, p. 12, 2013.

elements should be included. The Guidelines are developed through a global multi-stakeholder process involving representatives from different areas engaged in the activities and processes of an organisation: business, labour, civil society and financial markets, as well as auditors and experts in various fields.

In this regard, Guthrie et al. proposed a study underlining that according to the legitimacy theory a sort of "social contract" exists between the firm and the society in which it is rooted.[62] This ideal social contract regulates the behaviour of the company and establishes how it must act in compliance with the society's expectations and values. Thus, an adequate amount of disclosure that evidences how the firm is fully involved in addressing social and environmental issues according to socially acceptable behaviours established by the society is a useful tool for satisfying the society's expectations and information needs.

In concrete GRI provides a framework, to which companies can adhere voluntarily in order to produce sustainability reports, which *"should provide a balanced and reasonable representation of the sustainability performance of a reporting organization – including both positive and negative contributions".*[63] Sustainability reports allow companies to demonstrate that they are socially responsible and are a powerful tool for improving communication with stakeholder groups by enhancing the transparency and accountability of non-financial information.

The contribution provided by GRI has been without doubt crucial for creating a milestone in sustainable reporting; it also enhanced the credibility of this topic, trying to create a model for organisations, to deal with the urgency of sustainable development. However, producing a sustainability report besides the key financial statement shows some limitations, which are the following:

- Stakeholders tend to perceive a low reliability in reports produced on a voluntary basis according to guidelines not approved nor shared by the legislation, for this reason information disclosed by these reports is subject to scepticism.
- Very often, sustainability reports tend to be not aligned with financial performance, so in some cases it could be ineffective to evaluate a very positive sustainability report in relation to poor financial performances from the same organisation.
- Also a problem of comparability arises, since GRI guidelines are not mandatory and allow for some exceptions; for example an organisation could decide not to disclose a

[62] Guthrie, J.; Petty, R.; Ricceri, F. *The voluntary reporting of intellectual capital: Comparing evidence fromHong Kong and Australia*. J. Intellect. Cap., Vol. 7, pp. 254–271, 2006.

[63] GRI, Sustainability Reporting Guidelines G3, p.3, 2006.

specific piece of information because it could claim that a required disclosure doesn't apply to it or maybe the requested information is confidential. In this way, comparing sustainability reports across companies, or across time in the same company, becomes difficult.

- Sustainability reporting is also exposed to very low assurance level: it is very difficult to evaluate and audit documents reporting information disclosed on voluntary basis according to a framework or guidelines provided by an independent entity. Furthermore, the risk of "green washing" is very high, because companies could decide to alter or disclose only selected information to show a sustainable nature, which is actually not consistent with their performance. Consistently, as argued by Patten and Zhao in a research published in 2014, the use of a standalone sustainability report can be criticized because it represents *"an exercise designed not for transparent accountability, but instead for nothing more than image enhancement."*[64]

It must be highlighted that directives concerning non-financial information and its disclosure exist, the directive 2014/95/EU (in Italy, as in other member states, the regulations included in the directive became effective starting from 2017, in order to give the possibility to national jurisdictions to introduce such directive and organize related norms related to it) represents a revolution in the field of business reporting, since it is the fist mandatory regulation in the European Union referred to non-financial disclosure. However, in the directive it has been specified that non-financial disclosure implies at least information pertaining to environment, society, employers, human rights, fight against corruption and bribery. Hence, the directive does not trace a precise and unique definition of what is intended by "non-financial", instead it just limits to list some minimum requirements which must be included by organisations, to whom the directive applies, in their reports.

Once the European directive had been published, some researchers have started to investigate the level of compliance of annual reports with the directive issued by the European Commission. If we consider the Italian scenario, in 2017 Venturelli[65] focused on a sample of 223 large companies considered entities of public interest, analysing non-financial information disclosed in the mandatory and voluntary reports for the year 2015 and identified a medium level of compliance. In particular, the highest levels of compliance were

[64] Patten D.M. and Zhao N., *Standalone CSR reporting by U.S. retail companies*, Accounting Forum, Vol. 38, pp. 132–144, 2014.

[65] Venturelli A., Caputo F., Cosma S., Leopizzi R., Pizzi S., *Directive 2014/95/EU: Are Italian Companies Already Compliant?*, Sustainability, 9, 1385, 2017.

achieved with regard to two content elements: business model and sustainability policies; on the other hand, there was an insufficient level of compliance regarding diversity policies.

As mentioned above, this is the one of the reasons that pushed an organisation such as GRI to elaborate and produce some guidelines, which could lead companies to a correct and effective reporting of non-financial information.

The ultimate reporting form that has been presented in the business landscape is the framework provided by the International Integrated Reporting Council, which is a global coalition of regulators, investors, companies, standard setters, accounting professionals and NGOs. This organisation was founded at the end of 2010 with the aim of *"promoting communication about value creation, preservation and erosion as the next step in the evolution of corporate reporting"*[66]. IIRC published its framework on how to prepare an integrated report in 2013 based on seven guiding principles and eight content elements, with the main objective of communicating how the company created, preserved and transferred value over time. The new frontier of reporting proposed by IIRC focuses on value creation and on the disclosure of information concerning what is the value created and how it has been created.

The IIRC defines an integrated report as *"a concise communication about how an organization's strategy, governance, performance and prospects, in the context of its external environment, lead to the creation of value over the short, medium and long term."*[67] As in the case of GRI guidelines, whether to embrace the form of an integrated report or not is discretionary according to the will of organisations, except for South Africa, where listed companies must edit an integrated report.

Some criticism has been raised towards IR since it is focused on the concept of value to investors, mainly addressing the information needs of financial capitals providers. Moreover, in 2015, in one of its researches Flower blames the framework proposed by the IIRC as inconsistent, as it considers mainly the prosperity of the entity, rather than of the society.[68] Milne and Gray, commenting the IIRF, state: *"Despite its claims for sustainable development and sustainability, it is exclusively investor focused and it has virtually nothing—and certainly nothing substantive—to say about either accountability or sustainability"*.[69]

---

[66] www.integratedreporting.org

[67] IIRC Framework, p.10,2021.

[68] Flower J., *The international integrated reporting council: A story of failure*, Crit. Perspect. Account, 27, pp. 1–17, 2015.

[69] Milne M.J. and Gray R., *W(h)ither ecology? The triple bottom line, the global reporting initiative, and corporate sustainability reporting*, J. Bus. Ethics, 118, p. 20, 2013.

An integrated report should show a holistic picture of the combination, interrelatedness and dependencies between the factors that affect the organization's ability to create value over time. So basically, this integrated approach, known as "integrated thinking" in the framework is a basic concept on which integrated reporting funds. When the framework claims the importance of "connectivity of information" it actually means that all of the information disclosed in the report must be interrelated among the different topics and furthermore, the reporting activity should be a phase successive to the process of integrated thinking, during which the organisation establishes which activities, operations, capitals, aspects and issues are relevant to the creation of value of the firm and should be disclosed to providers of financial capital and stakeholders. Obviously, given the holistic approach of this type of report, non-financial information is a crucial part, which must be included in the document as indicated by the framework and contributes to the value creation process.

Moreover, among its content elements, the framework addresses attention to the issue represented by risks and opportunities. An integrated report identifies the key risks and opportunities that are specific to the organization, including those that relate to the organization's effects on, and the continued availability, quality and affordability of, relevant capitals in the short, medium and long term. This activity includes identifying the specific source of risks and opportunities, which can be internal, external or, commonly, a mix of the two, and assessing the likelihood that the risk or opportunity will actually present and the magnitude of its effect. This includes consideration of the specific circumstances that would cause the risk or opportunity to arise.

In other words, an integrated report groups the previous reports described (annual and sustainability report) into a single document after a process of evaluation and integration of all factors considered part of the value creation process for the firm. This approach demonstrates the holistic vision of the organisation, which has already been presented in the previous chapter, discussing about ERM and the framework proposed by COSO. In fact, it is possible to ascertain that the first two decades of the twenty-first century have been years of huge evolutions in the field of business management and reporting, even though with a common goal and perspective: reaching a more integrated vision and approach towards the way in which the organisation is managed and evaluated, internally but also by external parties with some interest in the activities of the company, trying to individuate and communicate the core elements involved in the value creation process.

4.2 Risk reporting: a focus on the disclosure of information concerning risks

The continual process of obtaining and sharing necessary information, from both internal and external sources, which flows up, down and across the organization, is an essential phase during the management of an enterprise. Also in the ERM framework proposed by the COSO in 2017 "Information, Communication and Reporting" is represented as one of the five main interrelated components, described as a fundamental phase during which investors get constantly informed on the risks faced by the company, in order to allow them to make correct and informed decisions. Communication plays a crucial role in the correct functioning of an efficient capital market, in particular way in the resource allocation process; this phase could be easily influenced and biased by some information issues depending on their availability and reliability.

The first problem which may verify, arises from the awareness that entrepreneurs, or more in general the individuals governing and running the business, found themselves in a privileged position with respect to the rest of the market, when it comes to the level and quality of information concerning the value of potential investments. Furthermore, entrepreneurs may decide to disclose information only partially and very often their personal evaluation of the company and investments in the company are generally overestimated. The consequence is that ex ante information asymmetries arise among the company and investors, who aren't able to carry out correct evaluations, since they lack all the necessary information. Such information asymmetry in literature is also known as "lemon problem"[70].

Information can be considered as a fundamental resource, so there is a conflict of interest verifying between the company, which acts in an opportunistic way (moral hazard) by not communicating the complete information, and potential investors, who are offered low quality opportunities at an elevated cost. In this case of adverse selection occurs: buyers, knowing that they own only part of the information, assign an average price to all goods, undervaluing the best opportunities and overvaluing the worst ones. A possible solution to this conflict of interest could be the stipulation of contracts between investors and entrepreneurs, in order for these last ones to be more incentivised to enhance information disclosure to mitigate the issues connected to wrong evaluations.

The second problem linked to a correct allocation of resources refers to agency problem that is an information asymmetry ex post between the enterprise and current investors. This kind of problem arises between the principal, who is the shareholder, and the agent, who is the

[70] This term has been introduced by Akerlof in 1970 in *"The market for "lemons": quality uncertainty and the market mechanism"* to indicate low quality goods, which real characteristics are known only by the vendor.

manager; this last party involved exercises a service for the principal, which consists in the delegation of some decisional power. Agency problems could verify during situations in which the managers don't operate in the interest of shareholders, trying to maximize their return. In order to mitigate the negative effects of these issues, there are different solutions such as signalling theories or the creation of institutions finalized at simplifying the interaction and communication between managers and shareholders.

Such types of solutions are also useful referring to risk reporting: as we have seen in the previous chapter, an increased disclosure of risks faced by the company leads to a decrease in the cost of capital. This theory has been first supported by researches conducted by Lang and Lundholm in 1996[71] and Botosan in 1997[72].

An effective communication concerning the risks to which the company is exposed has a strong impact on the strategies set by the firm and on the opportunities emerging. In fact, stakeholders and investors ask for information concerning future perspectives and the sustainability of other factors involved in the long-term value creation process.

The pressure for a greater disclosure derives also from the fact that annual reports are backward oriented, focusing on past results; however stakeholders and investors are more interested in forward looking information concerning future initiatives and projects, in order to evaluate future potential performances and evaluate whether the organisation owns the characteristics necessary to ensure the expected return on their investment.

The objective of risk reporting should be to fill the informative gaps between the organisation and the market, allowing potential investors to estimate future performance with more reliability.

Information concerning enterprise risks is part of the entire financial disclosure finalised at informing stakeholders on the current situation of the company, but most important on the future perspectives and on the risks faced by the entity in carrying out its activities.

A risk report is a document that discloses information about the company's most pressing risks; typically it will address the most critical risks, where consequences for the firm could be very severe, as well as emerging risks that could cause larger trouble in the future if they're not monitored carefully. Moreover, risks reports should also discuss how well the company is or is not managing those risks; so the report could also include material related to the policies and controls implemented by the company, reporting which ones are working and which ones

[71] Lang M. and Lundholm R., *Corporate disclosure policy and analyst behaviour,* The Accounting Review, 71, pp.467-490, 1996.
[72] Botosan C., *Disclosure level and cost of equity capital*, The Accounting Review, 72, 3, pp.323-345, 1997.

not, or what additional steps are necessary in order to keep risk level within the tolerance of the organisation.

Risk reporting is an important activity because internal policies may be insufficient and one of the jobs of the managers is to monitor the effectiveness of the risk management systems; and this monitoring activity cannot be carried out effectively without a deep understanding of what risks the company is actually facing. Another factor, which makes risk reporting important, is the strategic implication within the risks to which the company is exposed. Actually risk reporting supports the board in strategic advice: it may warn about upcoming risks or potentially dangerous situations which can verify in case of certain decisions, in this way managers can use risk reports as tools to ponder choices and support decision-making processes. Effective risk reporting is also important for regulators, whose job is to verify the company's conduct and review its compliance to rules imposed by superior institutions, and a scarce ability of the organisation to report and discuss risks is a sign of weakness of the company. A clear example can be observed in the EU directive 95/2014: in the second part of the text of the directive it is specified that bog size companies should disclose also the main risks connected to non-financial aspects involved in the company's activities and on the relative management processes implemented. So, it is clear that a lack of risk reporting, in case of European organisations, reflects into a lack of compliance to this directive, which in turn causes major strategic and operational consequences for the management.

Information concerning risks, which companies are required to disclose, are disciplined by different institutions in different contexts, especially if we consider different cultures such as the US and European countries. In the United States risk disclosure is regulated by the Securities Exchange Commission (SEC), in Europe instead we have different directives regulating the topic of risk disclosure.

However, there are some elements in common between the risk reports of organisations from different countries and legislations. As mentioned above, risk reports should address the most critical risks to the company, as well as the emerging risks, in order to provide a complete frame of what situations can be threatening for the company and which ones can represent a source of opportunities. Among the advantages recognised to risk reporting we can highlight two main ones:

- First of all, information concerning risks is expected to be long-term oriented since it looks at the future; investors and stakeholders are more interested in expected results of the organisation instead of historical data on past performance. Through risk reports investors are able to evaluate more accurately if the management of the

company is efficient and consistent enough to guarantee the desired return on the initial investment.

- Secondly, as mentioned above, a dynamic and careful management of risks results in a direct impact on cost of debt: increasing leverage could be more inexpensive because the lender is better informed on the company's risks and their management, hence has greater trust in the economic activities of the entity.

Also the models of risk reporting faced different phases in their evolution: initially annual reports provided very few information concerning risks faced by the organisation, without any mention to management models. In the years following the economic crisis and with an increase in the number of financial tools, informative needs of stakeholders changed radically, in fact they require companies to implement integrated risk management systems with a consistent disclosure of information from both a qualitative and quantitative point of view. Disclosure should address the potential sources of threats, different type of risks to which the company is exposed, subjects involved in the risk management systems, the activities implemented to mitigate risks and the responses planned to react to these risks and the consequences of risks of the situation of the enterprise. The main differences between a traditional risk reporting model and an evolved one are shown below[73]:

- The advanced model of risk reporting focuses on the future, disclosing information which is going to be helpful for forward-oriented performance, instead of focusing on historical information concerning the past results of the company;
- Evolved risk reports will present information concerning risks from a quantitative point of view based on frameworks and specific evaluations, followed by qualitative descriptions;
- The advanced model of reporting include details on the types of risks to which the company is exposed, quantifies the level of exposure to these risks and focuses on the management procedures of each category of risk, in the past instead risk reports simply reported vague and limited information concerning the main risks faced by the firm without any detailed description nor any references on the impact of such risks on the performance of the organisation;
- Data provided in the traditional reports were based on the accounting system, nowadays data relies on the information provided by the managerial system, which integrates all of the activities and operations inside the firm;

[73] Dicuonzo G., *La disclosure sui rischi finanziari tra dottrina, normativa e prassi, Evidenze empiriche dal contesto italiano*, p.49, G. Giappichelli Editore, Torino, 2018.

- Current corporate reports include specific areas reserved for disclosure of information on risks and risk management, in the past instead information on this topic were scattered in the financial statements when not totally absent.

A lot of studies on risk reporting have been conducted since the first institution dedicated to the development of risk disclosure has been funded in 1997: Institute of Chartered Accountants in England and Wales (ICAEW).

Most evidence regarding whether risk disclosure is actually consistent and informative for shareholders has been gathered through researches conducted in the US and the UK. Kravet and Muslus's in 2013[74] are among the first to test for the informativeness for narrative disclosures, investigating how changes in risk disclosure are related to changes in investors and analysts' activities. Their findings support the so called "divergence argument", implying that risk disclosure is informative; however in their sample the stronger relations emerged between industry-level risk disclosure and investors' perception of risk than for firm-level disclosure. This outcome actually supports the criticisms expressed by Kaplan (2011)[75], according to whom company specific risk information is actually lacking in annual reports, as we mentioned in the initial considerations on risk reporting.

Another research non-US-based has been proposed by Abraham and Shrives (2014)[76] whose aim was to measure the quality of risk disclosure as a function of three elements: specificity of risk factor disclosure for the company, regular evaluation of risk disclosures by managers identifying significant events ex ante to avoid redundancies and discussion upon the risks actually faced by the organisation. In line with prior works, the authors claim that risk disclosure provided by companies is actually non-specific and this fact limits its usefulness. Companies provide a large quantity of information, which is general rather than specific, hence providing *"more symbolic disclosure than substantive".* A lack of progression and evolution in disclosure may indicate a failure to adapt reporting to specific circumstances and situations.

Another theme that has been debated regards the importance of the relationship between informativeness and managerial incentives. The first one to analyse this topic was Campbell

---

[74] Kravet T. & Muslu V., *Textual risk disclosures and investors' risk perceptions*, Review of Accounting Studies, 18(4), pp. 1088-1122, 2013.

[75] Kaplan R. S., *Accounting scholarship that advances professional knowledge and practice*, The Accounting Review, 86(2), pp. 367-383, 2011.

[76] Abraham S. & Shrives P. J., *Improving the relevance of risk factor disclosure in corporate annual reports*, The British Accounting Review, 46(1), pp. 91-107, 2014.

in 2014[77], who actually concluded that, in contrast with Abraham and Shrives (2014), managers provide risk information which is meaningful according to the specific risks that their firms are exposed to, furthermore changes in risk disclosure influence investors' assessment of the risks faced by the organisation, but most importantly the value generated. Elshandidy and Neri (2015)[78] proposed another interesting study conducted on a sample of non-financial firms in UK and Italy. The authors examined how corporate governance influences the decision of the firm to disclose information on a mandatory or voluntary basis. The results showed that corporate governance factors are more related with voluntary disclosure among UK firms, instead they are more strongly associated with mandatory disclosure in Italian firms. It has also been highlighted how voluntary disclosure has a stronger positive correlation with market liquidity, as a proof of the fact that more informed the investors are, greater confidence in business evaluations and reliability can be established.

In synthesis, the value creation process for an organisation can be enhanced by an effective communication, since it is this practice's aim to satisfy the informative needs of stakeholders and potential investors. Furthermore, risk disclosure has also the objective of supporting the board in the surveillance of risks by providing updated information, which can help report's users to understand and evaluate connected risks, effects of risks on the financial position of the company and the management strategies of business risks.

This evolved model of reporting, which includes non-financial disclosure and in particular way the disclosure of non-financial risks to which the company is exposed, tries to respond to the continuously growing needs of knowledge showed by stakeholders on the topic of non-financial information, focused on future performance.

[77] Campbell J. L., Chen H., Dhaliwal D. S., Lu H. & Steele L. B., *The information content of mandatory risk factor disclosure in corporate filings*, Review of Accounting Studies, 19(1), pp. 396-455, 2014.

[78] Elshandidy T. & Neri L., *Corporate governance, risk reporting practices, and market liquidity: Comparative evidence from the UK and Italy*, Corporate Governance: An International Review, 23(4), pp. 331-356, 2015.

4.3 Thinking strategically: the importance of stakeholders' engagement

In the previous paragraphs the discussion regarding reporting and disclosure of non-financial information involved frequently the topic of stakeholders, in particular way the attention towards the provision of high levels of information concerning the organisation's operations to favour the parity of information among stakeholders and the board. The term "stakeholders" include a big variety of categories, from the ones internal to the organization (e.g. investors, employees, shareholders), to the ones found in the external environment (e.g. suppliers, customers, potential customers, governments, regulators).

Specifically, stakeholders are *"those groups who affect and/or could be affected by an organisation's activities, products or services and associated performance. This does not include all those who may have knowledge of or views about the organisation. Organisations will have many stakeholders, each with distinct types and levels of involvement, and often with diverse and sometimes conflicting interests and concerns."*[79]

In order to fully satisfy stakeholders' expectations in terms of information it is crucial for an organisation to engage with its stakeholders to understand and respond to their concerns. The increasing attention towards the relationship with stakeholders can be justified by the growing pressure exercised by them, in particular way for non-financial issues, which represent for the companies one of the most critical aspects, also in terms of disclosure. Under this perspective, stakeholders' engagement represents one of the main mechanisms that companies may implement in order to improve the management of non-financial issues and the disclosure of non-financial information. As it has already been pointed out, involvement of stakeholders in the processes of the organisation is of vital importance for the reporting procedures of the company; in fact stakeholder engagement is a main element in the frameworks provided by GRI and the IIRC.

Stakeholder engagement is defined as *"the process used by an organisation to engage relevant stakeholders for a purpose to achieve accepted outcomes"*[80] and is the result of an integrated thinking approach adopted by the company. In terms of value creation, thinking in an integrated way under a strategic perspective becomes crucial for the achievement of the objectives set by an organisation and for fulfilment of performance goals. Integrated thinking is an approach implemented with the aim of having an holistic vision of the organisation: the

---

[79] Definition provided by AA1000 Stakeholder Engagement Standard 2018, AccountAbility, 2018.

[80] Ibidem

complete picture of the activities, of the processes and the culture embedded in the company's mind-set gives the opportunity to the management team to connect the information inside the company and individuate the key areas to manage and improve in order to boost performance. Moreover, this approach of interrelatedness and dependency between key factors that affect the ability of the company to create value reflects also in the identification of main stakeholders, playing a central role in the value creation process.

It must be precised that literature provided a distinction between stakeholder engagement and stakeholder management. Stakeholder management is mainly focused in identifying and understanding requests, expectations and preferences of the different categories of stakeholders, in order to enhance the management of information disclosure to avoid conflicts of interests and asymmetries. On the other hand, stakeholder engagement goes beyond the share of information between company and stakeholders, this two parties discuss, compare among each other and generally stakeholders give advice on how the company can improve in fields of interests of the parties involved and be more transparent in disclosing information.

First of all, the company must define who are the key stakeholders, because only active categories in the interactions with the firm participate to the value creation process, secondary stakeholders extraneous to the activities and uninvolved with the firm's outcomes should be excluded. The engagement of "key" stakeholders is a concept that must be stressed, because it has deep roots in the strategic thinking approach. The organisation identifies and addresses the most material aspects related to its business and operations, which means that only issues and activities having a consistent impact on the value creation process of the organisation should be taken under consideration, processed and disclosed to users. This is the essence of one of the main concepts on which the IIRC based its framework of integrated reporting: materiality. In simple terms, a company should disclose information concerning financial and non-financial issues, given that these ones are central to the company's activities and their impacts have consequences on the ability of the firm to create, preserve and disclose value. As the organisation aims at identifying and evaluating only "material" aspects for disclosure, also in stakeholder engagement the company tries to select those categories subject to these main impacts provoked by the firm's operations. Similarly, the organisation identifies and addresses those categories of stakeholders with significant potential to influence the organisation, in terms of activities, performance, risks and opportunities.

Once key players have been identified, the organisation must disclose information concerning the relations with such stakeholders and in particular way, it should explain them how the company aims at addressing, evaluating and responding to their needs and interests. It is

important to stress the idea that stakeholder engagement doesn't mean only sharing information with the company and vice versa, stakeholder engagement consists in a consistent dialogue between parties in order to actively involve stakeholders in the decision-making processes of the firm. The approach of the company should overcome the idea of involving stakeholders as passive observers and users of information, instead it should entertain a dynamic and supportive relationship, in which key stakeholders collaborate with the company in order to align values and expectations with the ones of the company and lead to a strategic innovation of the processes and activities.

An integrated approach to management and reporting leads to perceive stakeholders as an essential resource to: understand stakeholder's perception of value, identify upcoming trends for the future, identify risks and opportunities, and enhance risk management. The logic behind integrated thinking, which has been the engine pushing IIRC to the creation and development of an Integrated Report Framework, incorporates the mind-set of integration and engagement of stakeholders playing a key role in the company's activities, even though in many cases these categories of individuals are external to the firm.

Having identified the scope and the purpose pushing towards stakeholder engagement, the company should implement a consistent stakeholder engagement process. In literature there are various frameworks and manuals describing how to conduct an engagement process with stakeholders, however in this case the point of reference is going to be the process provided by the global consulting and standards firm AccountAbility, which works with businesses, investors, governments, and multi-lateral organizations on ESG matters to achieve opportunities, advance responsible business practices, and transform their long-term performance. The engagement process is described in the manual "AA1000 Stakeholder Engagement Standard" published in 2015, which represents a milestone on which companies all over the world rely to guide their approach to sustainability strategy, governance, and operations management.

The engagement process includes four stages: plan; prepare; implement; act, review and improve.[81]

1. Plan

During this first phase, the company should profile and map the stakeholders they want to engage with by establishing a methodology, which shall be reviewed and revised throughout the whole process. Managers shall determine the levels and methods of engaging with key

[81] AccountAbility, *AA1000 Stakeholder Engagement Standard*, pp. 19-32, 2015.

stakeholders, who are best suited to the purpose and final aim of the engagement, but more in general with the scope of the company. Once key stakeholders and engagement process have been defined, the company must set the boundaries of disclosure, specifying what information are going to be shared with stakeholders involved in the process and what information may be shared outside the boundaries of the organisation. Finally, managers should prepare an engagement plan, which should be made available to stakeholders in order for them to provide inputs into the plan. Along with the plan, generally indicators for the quality of stakeholder engagement are established, in order to evaluate the effectiveness of the process and to measure the consequences of it on the general performance of the company.

2. Prepare

The company should identify and gain approval for the resources required for carrying out the engagement process successfully, such as financial, human and technological resources. Once resources have been identified and saved, the company and stakeholders involved in engagement should identify in which areas of the company engagement needs to be built and addressed; in some cases also external parties may be involved, if this benefits the whole engagement process. Besides the resources needed and where to allocate these resources, the organisation must consider the risks connected to the engagement process, so a consistent risk assessment framework or procedure should be implemented, coherently with the risk management system and approach of the company. Risks from the point of view of the company may include: reputational damage, loss of control over some issues, creation of conflicts of interest, non-compliance with internal policies and regulations or simply waste of resources (financial and of time).

3. Implement

This is the most practical phase of the process: the company must make sure that key stakeholders are invited to participate to the engagement plan and that communications are clear and appropriate for each stakeholder. In order to ensure a correct invitation and to obtain a positive feedback, the organisation must provide to all stakeholders involved with the briefing materials needed to ensure the success of the process. These materials should include the purpose and the scope of the engagement, the reason which pushed the company towards such decision, the nature of the issues in which stakeholders are going to be involved and what are the expectations, in terms of results, performance and value creation, for the collaboration between the organisation itself and all the other parties involved. The framework proposed by AccountAbility also specifies the importance of a set of ground rules, upon which all participants must agree, regulating and governing discussions between

parties. Documentation concerning the engagement and the outcomes must be reported and stored, in order for the organisation to analyse it and develop eventual plans or responses to improve the process and enhance efficiency. In a second phase, plans and outputs should be communicated to the participants of the engagement, also to avoid any information asymmetry.

4. Act, Review and Improve

This last phase of the process expects the organisation to systematically monitor and evaluate the general quality of the engagement process, just as the stakeholders involved should individually evaluate the quality of the engagement process. Evaluations should include: commitment and integration, purpose, scope and participation, process, outputs and reporting. The scope of monitoring and reviewing the process is to continuously try to improve the stakeholder engagement, developing actions plans in order for the organisation to become more successful as a result of continuous interactions. The company should publicly report the outcomes and impacts of the engagement activities, to show how the integration of stakeholders in the processes of the business contributes in creating value.

Even though the engagement process is not simple to implement and may be very costly in terms f resource of all kind, there are several benefits deriving from a positive and consistent engagement activity. For sure, an effective and strategically aligned stakeholder engagement can lead to more sustainable social development, giving the opportunity to many different parties involved or influenced with the activities of an organisation to give their opinion and be considered in decision-making processes. The reputation of the company is going to increase and the management of risks and opportunities is going to be more effective; furthermore cooperation among a company and its stakeholders allows to pool resources for problem-solving and improving performance, due to the share of a set of information and abilities which would remain unexploited without an engagement plan. Moreover, from a human and ethical point of view, stakeholder engagement helps to create a better relationship between the company and stakeholders, parties are going to trust more each other if they are used to work together and involve each other, with the common goal of generating and preserving value; because, as it has been highlighted several times, the outcomes and the results obtained by an organisation have direct or indirect consequences on its stakeholders, which sooner or later are going to impact them, and if the two parties keep working on their own without a consistent plan of information disclosure, risks threatening the firm and external parties may materialize and destroy value from both parts.

Another aspect of stakeholder engagement deals with the importance of making an effort to understand the interests and concerns of stakeholders unable to express their interests, such as future generations, discriminated or marginalized groups. Anticipating their needs and their concerns could give a huge advantage in terms of opportunities exploitation to an organisation and could lead to a series of proactive approaches, which may give the company a competitive advantage in terms of value creation in the business environment.

4.4 Mandatory and voluntary perspective of non-financial risks disclosure

Non-financial risks disclosure assumes a double nature: it can be voluntary, as it has been for many years, so basically it depends only on the willingness of the organisation whether to disclose information concerning non-financial activities and risks or not, or it can be mandatory, so companies have no discretion in deciding whether to disclose information regarding non-financial aspects because it is the law which imposes specific regulations and policies to comply with.

In the past years the lack of specific regulations concerning communication on risks encouraged the disclosure of information on a voluntary basis, however this discretion created asymmetries in risk disclosure procedures adopted by different companies. Institutions releasing regulations, in order to favour comparability among reports and to ensure greater transparency in terms of communication with stakeholders, decided to introduce specific norms and standards concerning risk disclosure.

Referring to non-financial disclosure, the greatest break in the European Union between voluntary and mandatory disclosure is represented by the Non-Financial Reporting Directive (NFRD), also known as Directive 2014/95/EU. Among the different topics on which large companies are obliged to disclose there are: environmental matters, social matters and treatment of employees, respect for human rights, anti-corruption and bribery, diversity on company boards (in terms of age, gender, educational and professional background). Not only information concerning the topics listed above must be disclosed, but also information concerning the risks emerging from these themes, which the companies are going to deal with.

From a theoretical point of view, voluntary disclosure is the consequence of an arbitrary decision taken by the organisation to disclose additional information with respect to the minimum imposed by the law. For companies facing big growth opportunities, very often mandatory communication is insufficient and information asymmetry between managers and the market is quite consistent. Voluntary disclosure aims at mitigating such asymmetry and providing a higher quality of information for the investors to rely on, in order to make better-informed decisions, incentivizing investment. There are different theories justifying a voluntary approach, based on the information asymmetry issue, especially if we consider communication upon risks, anyway, these theories are going to be discussed in the following paragraph.

Along with the development history of non-financial information disclosure, accounting literature originally focused on voluntary non-financial information disclosure and the effects proven by such approach.

These studies demonstrated that voluntary non-financial disclosure enhances transparency, improves reputation and brand value (Hahn and Kühnen, 2013)[82], affects firm value, increases share prices (Cahan et al., 2016)[83] and reduce the cost of capital (Dhaliwal et al., 2012)[84]. More specifically, higher levels of disclosure on sustainability aspects lead to lower equity costs, and such reductions can be explained by the decrease of asymmetric information among parties. Martínez-Ferrero, Ruiz- Cano and García-Sánchez, in a study conducted in 2016[85], confirm that the reduction of asymmetry information plays a crucial role in the sense that non-financial disclosure quality reduces the cost of capital by decreasing information asymmetry; hence firms that promote non-financial disclosure, for an information asymmetry reduction objective, achieve lower capital costs.

According to a research conducted by Beck C., Dumay J. and Frost G. in 2017, the increase of sustainability reporting practices has raised the pressure for regulatory adequacy to ensure consistent comparability of data provided by organisations; hence, accounting research has started investigating mandatory regimes of non-financial information disclosure.[86] A compulsory approach to disclosure provides greater data comparability as well as the standardised and transparent ways for analysing companies' social and environmental impacts.

Mandatory disclosure is constituted by the set of information disclosed by the organisation, which have to comply with existing regulations imposed by the law. Authorities decided to introduce these limits and obligations mainly to create positive effects linked to a consistent informative flow. A positive effect of mandatory disclosure is the fact that investors find themselves in an optimal position to evaluate investments: the capital market is not perfect

---

[82] Hahn R. and Kuhnen M., *Determinants of sustainability reporting: a review of results, trends, theory, andopportunities in an expanding field of research*, Journal of cleaner production, 59, pp. 5-21, 2013.

[83] Cahan S. et al., *Are CSR disclosures value relevant? Cross-country evidence*, European Accounting Review, 25(3), pp. 579-611, 2016.

[84] Dhaliwal D.S. et al., *Nonfinancial disclosure and analyst forecast accuracy: International evidence on corporate social responsibility disclosure*, Accounting Review, 87(3), pp. 723-759, 2012.

[85] Martinez-FerreroJ., Ruiz-Cano D., Garcia-Sanchez I.M., *The Causal Link between Sustainable Disclosure and Information Asymmetry: The Moderating Role of the Stakeholder Protection Context*, Corporate Social Responsibility and Environmental Management, 23(5), pp. 319-332, 2016.

[86] Beck C., Dumay J., Frost G., *In Pursuit of a "Single Source of Truth": from Threatened Legitimacy to Integrated Reporting*, Journal of Business Ethics, 141(1), pp. 191-205, 2017.

and one of these imperfections is represented by information asymmetry, in fact authorities intervene to mitigate the fact that companies are more informed than investors, who are the ones having to take a decision whether to invest or not. So basically mandatory regulation on disclosure gave the possibility to investors to receive higher level of information to conduct their analysis and decide whether to invest in a company or not. Another positive effect of mandatory disclosure is the increase of overall economic wealth of the system: the reduction in the information asymmetries between organisations and investors benefit also the community. The mandatory character of disclosure benefits the entire collective, because costs related to disclosure and communication borne by the organisation are lower than the ones that should be borne by external subjects. Furthermore, it has been observed that information disclosed in compliance to regulations, benefit greater reliability in the market, because the presence of auditors, internal and external, aimed at verifying the truthfulness of information discourage managers to act opportunistically or in a way that could damage the company.

However, mandatory disclosure is costly in terms of resources and time, in fact, it is not feasible to introduce regulations and policies unlimitedly, it is necessary that companies continue to disclose voluntarily information for three main reasons[87]:

- Organisation bear costs, implicitly and explicitly, in order to produce and disclose information, these costs increase in case of excessive regulation governing disclosure;
- An excessive flow of information due to compliance with laws can destabilize the market with a consequential increase in the volatility of stocks and riskiness;
- If too many information are provided to the market, there is the risk of greater confusion and as a consequence more difficulties in selecting key information crucial for decision-making processes of investors.

Moreover, mandatory requirements on disclosure imply high costs of monitoring and reporting, which may overcome the expected benefits and, eventually, result even higher than the costs involved in a voluntary regime. Hence, these high costs can produce a counterproductive effect if companies do not provide extensive requirements, which will consequently cause an inverse effect with respect to the desired one: compliance with disclosure rules is going to be treated as a mere duty to fulfil, without any strategic advantage

[87] Dicuonzo G., *La disclosure sui rischi finanziari tra dottrina, normativa e prassi, Evidenze empiriche dal contesto italiano*, G. Giappichelli Editore, Torino, 2018.

nor exploitation of opportunities which come along with disclosure activities, decreasing the level of disclosure or eventually shrinking the disclosure's quality.

From an empirical point of view, researches on risk disclosure are not concordant on results.

Some studies show that moving from a voluntary regime of disclosure to a mandatory one didn't imply any significant increase in the level of disclosure. Specifically, in 2005 Dobler conducted a study on some German companies, highlighting how the change towards a mandatory disclosure produced only a small increase of transparency in the reports.[88] This could be a consequence of the lack of expertise by managers, imprecise and vague rules regarding disclosure and a poor commitment by companies. The author argues that, since risk reporting is a subjective discipline, forward-oriented, hence not verifiable, and based on events that may occur or less, it is not coherent to expect that managers won't hide any important information even though regulations have been imposed. In 2008 Dobler conducted another study, claiming that mandatory disclosure doesn't avoid managers from selecting which information disclose to the market and which not, so the imposition of specific norms on disclosure isn't an aspect improving transparency of risk reports. According to the author, analytical model provide three explanations to the limited communication upon risks disclosed by companies:

- Managers do not disclose information concerning risks because they aren't informed enough in first person, even though a risk management system is implemented this doesn't mean that reporting on risks improves automatically,
- Managers do not disclose information available either because they aren't reliable enough or because they voluntarily decide non to disclose them;
- Managers may decide not to disclose any information concerning risks faced by the company and how these risks are managed in order to avoid a situation of competitive disadvantage for the organisation.

Other studies, instead, highlight the fact that since regulations on disclosure have been introduced the level of information provided to the market has increased. In particular way Miihkinen examined in 2012 the evolution faced by risk disclosure in the business reports in Finland, after the introduction of a new standard in 2006 by the Finnish Accounting Practice Board, which provides indications on the qualitative level of disclosure and on requirements

[88] Dobler M., *How Informative is Risk reporting? A Review of Disclosure Models*, Munich Business Research, Working Paper, n. 1, 2005.

to implement the standard.[89] In synthesis, after the framework has been published, the Finnish listed companies analysed showed an increase in the level of risk disclosure reported in the annual reports, with a greater emphasis on the qualitative information regarding the impacts of potential risks. Also information regarding future prospects and initiatives resulted in more detailed explanations. This study contributes in demonstrating that a detailed guidance on risk disclosure actually enhances the quality of reporting.

The more recent study by Gao F. (2016) is one of the first to examine the determinants and economic consequences of the change in non-financial disclosure quality within a mandatory approach.[90] Based on a sample of almost five hundred Dutch firms mandated to self-assess their non-financial disclosure, the study investigates whether or not disclosure quality can affect capital markets and whether or not capital markets are likely to accordingly differentiate in their quality of disclosure. The multiple rating score of the Ministry of Economic Affairs has proved the disclosure of non-financial information and the findings suggest that non-financial performance, financing needs, and corporate governance determine the quality of non-financial disclosure. Moreover, a higher quality of non-financial disclosure leads to greater analyst coverage, higher levels of institutional ownership, and greater stock liquidity.

Stubbs and Higgins in 2018 explored practitioners' preferences between mandatory and voluntary approaches for disclosure in integrated reporting, and the findings demonstrate that a voluntary approach towards reporting is greatly accepted due to its effectiveness during the early stages of implementation.[91] The underlying reason for this result may be attributed to the strong intrinsic intentions associated with addressing such responsibilities. However, it is also true that it might address a misleading evaluation from stakeholders or exponentially enhances green-washing behaviours, which occur when companies engage with non-financial practices to improve their image and reputation rhetorically but not in practice.

In synthesis, on one hand, mandatory disclosure may help stakeholders more thoroughly understand how companies perform in terms of long-term sustainability, while on the other hand, it may lead companies to adopt a mere duty without an end purpose and without exploiting the strategic opportunities lying in non-financial reporting.

---

[89] Miihkinen A., *What Drives Quality of Firm Risk Disclosure? The Impact of a National Disclosure Standard and Reporting Incentives under IFRS*, in "The International Journal of Accounting", vol. 47, n. 4, pp. 437-468, 2012.

[90] Gao F. Et al., *Determinants and Economic Consequences of Non-financial Disclosure Quality,* European Accounting Review. Taylor & Francis, 25(2), pp. 287-317, 2016.

[91] Stubbs W., Higgins C., *Stakeholders' Perspectives on the Role of Regulatory Reform in Integrated Reporting*, Journal of Business Ethics, Vol. 147(3), pp. 489-508, 2018.

4.5 Theories underlying the voluntary character of risk disclosure

In the previous paragraph the difference among mandatory and voluntary non-financial disclosure has been analysed and both positive and negative effects of these two approaches have been highlighted. In general we referred to non-financial disclosure, taking some studies as point of reference to understand what are the advantages and disadvantages of both perspectives; in the following paragraph the focus will move towards risk reporting, which is the main topic of this work, considering the impacts on disclosure and how stakeholders perceive the consistency of a risk report.

Given the growing importance of risk disclosure in terms of strategic advantage for the company, in order to attract new investors and gain competitive advantages in the market, organisations have to face the issue of the implementation of a voluntary risk disclosure. Even though regulations implied in accounting principles and business laws oblige to disclose certain type of information, there are some companies who evaluate the possibility of disclosing additional information with respect to the regulation. The reasons pushing organisations towards this decision can be justified and supported by different theories developed in literature; many studies focused on the analysis of the trade-offs existing between costs and benefits of communication upon risks, trying to identify the purpose according to which managers should decide to disclose information on a voluntary basis.

The different theories which are going to be proposed and observed divide themselves into two categories, according to the risk disclosure regime to which they apply: voluntary regime (a context in which the company is free to disclose any kind of information concerning risk) or interaction between mandatory and voluntary regime (a context regulated by norms and laws governing the discipline of risk disclosure, however organisations can decide to go into deeper details and provide more data according to their willingness).[92]

The following theories are going to be analysed:

- Signalling theory
- Legitimacy theory
- Agency theory
- Political costs theory
- Proprietary costs theory
- Institutional theory
- Interaction theory

[92] Panfilo S., *La gestione del rischio e la sua comunicazione. Gap teorici ed evidenze empiriche nelle società quotate italiane*, Aracne editrice, pp. 47-58, 2020.

Signalling theory

This theory has been developed by Spence in 1973, explaining that information disclosed by companies act as signals to the market, hence it can transfer further information regarding competences, performance and activities in order to influence evaluations and decisions taken by stakeholders. According to the signalling theory, organisations may be interested in providing additional information to stakeholders and investors if they can gain a consistent benefit from it, in terms perception of greater value generated by the company. The decision to send signals to stakeholders is also a strategic decision, since managers disclose the best performances of the organisation, showing the implementation of good practices of risk management, promoting transparency and attracting more investments. Under this perspective, information on risks faced by the company and how they are managed contribute to enhance the company's reputation among investors and can be used as a tool to boost the price of stocks in the market.

Legitimacy Theory

Legitimacy theory has been elaborated by Shocker and Sethi in 1974 and deals with the relationship between the organisation and the company. According to this theory there is a "social contract" existing among the company and the community, as a consequence both parties interact following specific shared rules. Not only companies must conduct their activities within the boundaries of this social contract, but they should also guarantee that their business activities reflect the expectations of stakeholders. If a company doesn't follow the terms of the contract, then it tries to remedy communicating to society additional information with respect to the original contract, to legitimize itself. This theory supports voluntary disclosure regime because the company could provide voluntarily specific information on aspects such as non-financial risk management in order to justify certain actions and reduce pressure exercised by the social context.

Agency Theory

This is one of the most diffused theories and has been introduced in 1976 by Jensen and Meckling to deal with the relationship between shareholders (principal) and managers (agent). Agency problem arise when both the principal and the agent want to maximize returns according to their interests, which are not aligned among them. Agents are going to act in an opportunistic way, creating problem of information asymmetry. In order to mitigate this problem, principals may implement some monitoring mechanisms to limit the power of managers and discourage them from acting in their own interests. Agency theory has been largely used when dealing with disclosure and characteristics of enterprise risk management.

Board of directors in fact are expected to supervise over risk and implement an ERM system able to enhance the monitoring activity over the whole organisation and to mitigate information asymmetry. Such monitoring systems support companies in supervising the attitude of managers upon risks and ensure consistent and appropriate flow of information concerning risk disclosure.

Political Costs Theory

Watts and Zimmerman are the founders of this theory, developed in 1978 and assuming that decisions taken by managers on accounting methods are influenced by political costs. According to this theory, some organisations attract more attention than others, especially large companies, and it is more likely that these companies take accounting decisions aimed at minimizing profits and disclosing more information than others trying to manipulate their image and reducing political costs. The purpose of this attitude is to avoid that wealth gets taken away from the company, as it is in the interests of both managers and shareholders. Political costs theory pushes companies to comply with requirements imposed by the law in terms of disclosure regulation, in order to reduce pressure from authorities and the public. The authors claim that companies more politically exposed than others should react to the policies imposed by the authorities by disclosing on a voluntary basis more information regarding risks than the ones required, to avoid that more detailed and costly requirements are introduced.

Proprietary Costs Theory

Proprietary costs theory has been developed in 1983 by Verrecchia and focuses on the trade-off between proprietary cots and competitive advantages. Proprietary costs include preparation costs, disclosure costs, assessment costs and competitive costs associated to the disclosure of sensitive information that could be used by competitors to damage the company itself. If costs outweigh benefits, than the threat of an economic damage may discourage voluntary risk disclosure. According to this theory, the incentive to increase disclosure above the legal requirements is negatively related to potential costs related to it and positively related to the advantages that may origin from it.

Institutional Theory

DiMaggio and Powell have elaborated this theory in 1983. The authors suggest that when organisations face increasing expectations, regulations and conceptual frameworks, some of them perceive the pressure to disclose information concerning the processes they have implemented to monitor risk, in order to show that they commit to satisfying expectations upon risk management. Institutional theory actually disincentives voluntary disclosure of

information relative to risk and it's management because existing regulations limit companies to simply implement minimum standards of monitoring, without any specific element which increases the quality of disclosure.

Interaction Theory

In a mandatory risk disclosure regime, in which voluntary disclosure interacts with the mandatory one, it is possible to identify two different hypothesis: one incentivises greater disclosure, the other disincentives it.

In 1986 Dye developed a "complementary hypothesis", according to which voluntary disclosure increases as mandatory disclosure required by authorities increases. This positive correlation arises from the assumption that an increase in regulations on disclosure supports and enhances credibility of information disclosed on a voluntary basis. In fact, managers are encouraged to disclose additional information to distinguish their companies on the market, with respect to others, in order to increase the market value of shares and, as a consequence, increase their wealth.

In 1988 Jung and Kwon, followed by Verrecchia in 1990, support a "substitution hypothesis". According to this theory new regulations imposed by authorities, hence increasing mandatory disclosure, oblige managers to comply with these rules and by doing so these ones feel entitled to reduce additional disclosure based on their willingness, because they perceive that the information gap existing between the organisation and stakeholders has been reduced. As a consequence, more detailed and strict regulations do not modify the level of information, because the quantity of information disclosed previously on a voluntary basis now is implied into reports, which by law are more detailed and specific.

Chapter 5

ERM process and strategy within a business: an empirical study

5.1 Definition of the research question: Do companies with a higher level of ERM and more sophisticated processes evaluate and disclose more relevant information concerning non-financial risks to stakeholders?

Enterprise risk management is a holistic process of business risks management, which involves the entire organisational structure and, if implemented in a coherent and effective way, it allows the organisation to realize its ultimate goal of creating and maximizing value for stakeholders.

In the previous chapters its has been explained the history of risk management and how ERM has been the natural response to the changes faced by the external environment from an historical, economic, environmental and social point of view. These factors induced organisations to shift from traditional risk management policies to a more integrated process, which required the direct involvement of all levels of the enterprise, especially the higher levels of governance, in order for the approach to be effective. Simultaneously to the development of the holistic vision of an ERM approach, this paper examined how the systems of ERM approach are linked to the aspect of non-financial information management and disclosure inside the company. In fact, the chapters following the first one aim at creating a path through the topic of ERM frameworks and management of non-financial risks, analysing the relevance of non-financial aspects and issues impacting on the overall performance of the organisation and observing the importance of non-financial disclosure in terms of stakeholder engagement and value creation process.

The most relevant studies on ERM have been published on accounting and finance journals and, more recently, on management and financial journals. This fact contributed to enhance the perception of the interdisciplinary nature of ERM, a field in constant flux to which authors continue to contribute through their researches and studies, even though they appear in conflict sometimes. *"This interdisciplinary appeal suggests that, depending on the hypothesis, ERM is a topic that can be studied from various business lenses".*[93]

[93] Iyer, S. R., Rogers, D. A., Simkins, B. J., & Fraser, J., *Academic research on enterprise risk management,* Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives (The Robert W. Kolb series in Finance), John Wiley & Sons, Inc., Hoboken, NJ, pp., 419-439, 2010.

In general, studies on ERM can be classified into four broad categories[94]:

- ERM implementation;
- Determinants of the ERM adoption;
- The effectiveness of the ERM process;
- Other aspects of ERM, such as ERM strategies, ERM maturity, the impact of the institutional context on ERM adoption or ERM as a moderating factor between different variables.

Acknowledged this fact, the following empirical analysis contributes to the academic research in an original way, trying to stress the concept of ERM as an interdisciplinary topic affecting the overall performance of an organisation.

This empirical study regards a sample of Italian listed companies because so far the context of investigation and precedent research focused mainly on US companies. The reason could be related to the fact that European companies, such as Italy, have a totally different composition of the proprietary asset and tend to finance their activities through classic options such as bank loans. Furthermore, very few evidence of the effects of ERM on the performance of the firm, on the level and quality of disclosure is known, since attention to risk management practices by corporate governance codes is quite recent and rarely company owners implement formal ERM systems, due to their tendency of exerting periodical stringent controls and monitoring activities.

The analysis will start from the level of implementation of enterprise risk management systems inside the companies involved in the study, and in order to do so the main tool which is going to allow gathering all the information required is the corporate governance report. The corporate governance report is one of the main compulsory documents provided along with the financial statement and prepared by the managers; it includes a statement of corporate governance procedures and compliance, information on board composition, statements on the company's performance, and information about compliance and conformance with best practices for good corporate governance. A corporate governance report should also include a statement of disclosure of the company's governance procedures and compliance, disclosing the principles and codes that guide the company's procedures. According to the Italian legislation (art. 6, comma 4, d.lgs. 175/2016) editing the corporate governance report is compulsory for listed companies and the document must also include a description of the main risks and uncertainties to which the company is exposed, for this

[94] Classification proposed by Sorin G. and Anca E., *Enterprise risk management: a literature review and agenda for future research*, Journal of Risk and Financial Management, Vol. 13 (281), pp. 9-15, 2020.

reason this type of document has been selected in order to find the information to understand what level of ERM is implemented in each company and how sophisticated the approach is.

The second part of the research will focus on the sustainability reports or non-financial statements produced by the organisations part of the sample, in order to verify how non-financial disclosure is organised and what kind of information are provided to stakeholders, starting from the most classical ESG aspects, up to disclosure concerning non-financial risks faced by the company and how managers plan to manage these threats, or eventually mitigate situations potentially harmful for the enterprise.

The originality of this empirical study, which should partially contribute to enrich the academic research on the topic of ERM, stands in observing the link between enterprise risk management and non-financial risks disclosure. The aim is to verify whether a sample of Italian listed companies with advanced systems of ERM actually are more sustainable and disclose to stakeholders greater information regarding the non-financial risks faced by their companies, with respect to another sample of Italian listed companies, which implemented ERM approaches in a less effective way, integrating only partially the processes of risk management with the strategies and the operations of the companies.

5.2 Description of the sample taken under examination

For greater consistency of results and coherence in evaluations, the companies selected for this study pertain all to the same industry, in order to better identify and understand the differences among the way business is conducted and to find a reliable answer to the initial research question.

For this reason, in order to answer to the research question established as starting point, the sample of companies to study pertains to the financial industry.

As anticipated above the research at issue focuses on the Italian perspective, specifically on companies listed in the FTSE MIB index, which is the most significant index of the Italian stock exchange market. Currently, forty companies pertaining to different industries compose the index, even though the one with the greatest number of representatives is the financial industry: 14 companies of the FTSE MIB index operate in the financial sector. The rest of the companies listed in the MIB index are fragmented into different industries, such as utilities, automotive, manufacturing and pharmaceutical.

The choice of analysing listed companies derives from different considerations. First of all, tracing information of listed companies is much easier and more immediate with respect to non-listed companies. In the second place, listed companies must comply with a series of regulations and fulfil duties, which provide the market with information enabling a more effective evaluation of the company itself, in addition to a greater disclosure of financial and non-financial issues. Since this research focuses on the relationship between the implementation of ERM approaches and the disclosure of information concerning non-financial risks, the choice of listed companies is almost mandatory: ERM is an approach embedded into the business culture which can be shared and implemented by an organisation or not according to the decisions of the board; on the other side non-financial information is still an hybrid topic due to the presence of some regulations imposing disclosure, but at the same time there is lack of frameworks, specific guidelines explaining exactly which data companies are expected to provide to the market and lack of assurance systems to verify the truthfulness and accuracy of non-financial reports.

5.3 Assumptions and methodology to conduct the study

A premise is necessary before the exploitation of the methodology implemented to conduct the study: the documents of the companies analysed in this research refer to the 3-year-period 2018, 2019 and 2020. The choice of analysing these three years has been dictated by the fact that the European directive EU 2014/95 became effective in all member states starting from 2017. Since this research focuses on the relation between ERM and non-financial risk disclosure, the fact that the years taken under consideration are subsequent to the legislation gives more consistency and solidity to the results. Before the implementation of the directive non-financial disclosure was characterised by the willingness of companies, which implies that information tends to be scarce and poorly detailed, instead since 2017 disclosure of non-financial statements for large companies became mandatory, so at least some minimum requirements must be fulfilled, which increases the level of information and the comparability among organisations.

The first step of the research consisted in selecting the pool of companies among which the sample to study has been chosen. The criterion of selection of the initial pool has been explained above, the following step is choosing the sample of three "best" and three "worst" companies to analyse, in terms of ERM approach. The first challenge is ranking the Italian listed companies according to the level of ERM implemented in their business and the strength of such approach in the timeframe considered. In order to classify the Italian listed companies operating in the financial industry, this study is going to investigate in detail the level of ERM integration in corporate governance for each company, adopting the methodology proposed by Professors Florio and Leoni (2017) in a research conducted on Italian listed companies, researching the positive relationships between ERM implementation and firm performance.[95]

The criteria emerged by the authors' research refer to a series of components signalling the risk management integration in corporate governance of the company and the risk assessment process, according to the corporate governance code directives disclosed by Borsa Italiana in the 2011 reform, aimed at encouraging the creation of an integrated system of internal control and risk management, *"designed as a system of rule, procedures and*

[95] Florio C. and Leoni G., *Enterprise risk management and firm performance: The Italian case*, The British Accounting Review, 49, pp. 56-74, 2017.

organizational bodies deputed to identify, measure, manage and monitor main risks"[96]. These components are the following.

- **Presence of a Chief Risk Officer (CRO)**: a manager responsible for identifying firm risks, for programming, executing and managing the internal control and risk management system, and for reporting timely on critical issues to the board and ICR committee;
- **Presence of an Internal Control Risk (ICR) Committee or Risk Committee**: or a specific risk committee besides the Internal Control committee with a risk advisory role in the board of directors about the Internal Control Risk Management system and the internal audit;
- **Reporting frequency between the ICR committee and the Board of Directors**: which shall be at least biannual according to the Italian CG code (2011);
- **Frequency of risk assessment**: according to COSO document "Risk Assessment in Practice" (2012)[97], risk assessment shall be carried out continually, at least with regard to the most dynamic risks, such as certain market and production risks;
- **Level of depth in the assessment**: as recommended by COSO, risk identification and assessment shall be executed at both the corporate level and business units, organising risks by category and sub-category;
- **Risk assessment methodology**: The COSO framework suggests that, after an initial qualitative risk screening, companies shall perform quantitative analysis on the most important risks.

Once the evaluation criteria have been set, the following step implies the research of these components in each company, through the study of the corporate governance report of the year 2018 (this year has been selected since it is the first of the three-year-period chosen to conduct this study, also the corporate governance reports of the remaining years are going to be assessed). The corporate governance report is a mandatory document to be disclosed by every listed company in Italy and containing the information regarding corporate governance and individual risk management approaches exerted by the organisation. For each component a dummy variable equal to 1 is derived if the corporate governance report fulfils the requirement of the underlying component, otherwise the company is going to receive a 0 on that specific item. At the end of the evaluations for each component, summing all of the

[96] Borsa Italiana, *Codice di Autodisciplina*, art. 7,P.1, 2011.

[97] https://www.coso.org/Documents/COSO-ERM-Risk-Assessment-in-Practice-Thought-Paper-October-2012.pdf

single variables' score, a comprehensive score is going to be derived, indicating the level of sophistication of the ERM system implemented by each organisation. If the comprehensive score is equal or greater than 4, the company is considered with an ERM system "advanced" and will receive a score equal to one derived from the use of a dummy variable, otherwise the company is evaluated as "poor" in its ERM activities and approach, so it will receive a zero.

Once the 14 companies have been evaluated, a group of "best" and one of "worst" is selected in order to proceed with the analysis.

In the second phase, the two samples are going to be observed under the non-financial perspective; more specifically, the focus moves towards the non-financial statements or sustainability reports of the triennium taken under analysis for each company, so that it could be examined in depth, assessing the information of non-financial character disclosed by each organization and evaluating the data concerning risk disclosure, in particular way those ones addressing non-financial aspects, other than the typical financial risks. The non-financial risk disclosure to which the research refers to, consists in the research inside the sustainability reports of information regarding the fourteen elements included at point seven of the 2014/95 EU directive, listed in the table 1 below.

TABLE 1 Detailed list of the NFI elements identified through the content analysis

Nonfinancial information		
Environmental	**Social**	**Governance**
1. Current and foreseeable impacts of the undertaking's operations on the environment and on health and safety (Impact)	6. Actions taken to ensure gender equality (Gender)	13. Instrument in place to fight corruption (Corruption)
2. Use of renewable and/or nonrenewable energy (Energy)	7. Implementation of fundamental conventions of the International Labor Organization, working conditions, social dialog (Dialog)	14. Instrument in place to fight bribery (Bribery)
3.Greenhouse gas emissions reduction strategy (Gas)	8. Respect for the right of workers to be informed and consulted (Workers)	
4. Water use (Water)	9. Respect for trade union rights (Trade Union)	
5. Air pollution (Air)	10. Health and safety at work (HS)	
	11. Dialog with local communities, and/or the actions taken to ensure the protection and the development of those communities (Local Community)	
	12. Respect for human rights and prevention of their abuses (Human Rights)	

Source: Mio, Fasan, Marcon and Panfilo, *Carrot or stick? An empirical analysis of the different implementation strategies of the EU directive on nonfinancial information across Europe*, Corporate Social Responsibility and Environmental Management, p. 6, 2021.

The research tries to analyse from a quantitative – NFR (qn) score - and qualitative – NFR (ql) - point of view the information concerning non-financial risks disclosed in the statements of each company, in order to understand which companies are providing more precise and consistent information to their stakeholders. The level of disclosure concerning non-financial risks is going to be measured through a score (NFR Score) comprehensive of both the quantitative and qualitative score attained by each company of the sample.

In order to determine the quantity of information concerning non-financial aspects disclosed, in particular way information upon risks faced and managed by the company at issue, a content analysis has been applied to identify different elements of non-financial nature. This approach takes inspiration from a prior analysis conducted in 2021 by Mio, Fasan, Marcon and Panfilo.[98] Even though the purpose of this study is different from the one of the authors above, the content analysis proposed in their work suits the quantitative analysis of this research. More specifically, the authors cited above analysed all kind of non-financial statements in order to organize the content according to the EU Directive 2014/95, which at point seven of the text lists a series of fourteen elements of environmental, social and governance nature to be mandatorily included into non-financial statements of large organisation which have to comply with the directive.

This empirical study aims at applying the same approach described above, in order to give a quantitative perspective to its analysis. However, instead of conducting a content analysis on non-financial issues, the attention is oriented towards the topic of non-financial risks. To check which companies disclose more information concerning non-financial risks, the research will focus on whether the sample of companies disclose explicitly information on risks concerning the fourteen elements listed in the directive or not. "Explicit information" is considered in such a way, if the report presents risks related to the information itself and related policies if any. In this way, it can be established which companies are more engaged with disclosure on non-financial risks and ought to inform stakeholders thoroughly. Also in this case the implementation of a dummy variable is adopted to assign a final score to each company in each year regarding their level of non-financial risks disclosure; 1 is going to be assigned in case the company discloses the information relative to the point of the directive at issue, otherwise the company will receive a 0. Obviously, given that the directive discusses fourteen points, fourteen is the maximum score, defined as NFR (qn) score, attainable by a single organisation. This systematic approach is going to be implemented for each year of the timeframe considered, in order to enhance comparability among years between the ERM score and the NFR score of each company.

For what concerns the qualitative aspect, the analysis will base its observations on four parameters discussed in existing literature, in order to give more consistency to a series of evaluations which otherwise may risk to be excessively subjective. These four qualitative variables can be summed up into: quantification, time orientation, tone and volume. All of

[98] Mio C, Fasan M, Marcon C, Panfilo S., *Carrot or stick? An empirical analysis of the different implementation strategies of the EU directive on nonfinancial information across Europe*, Corporate Social Responsibility and Environmental Management, pp. 1–15, 2021.

these variables evaluate from a qualitative perspective the amount of disclosure upon non-financial risks, which is provided by the companies taken under consideration. Each variable is going to receive a score for each year of the timeframe considered, which in the case of the first three is going to be derived from the implementation of a dummy variable, the last one is going to be expressed as a percentage.

In more details, quantification is a variable referring to the type of disclosure provided by the report, so whether the information related to non-financial risks is reported in a descriptive way or if there is any reference to numbers quantifying the risk faced by the organisation. In the first case, the score assigned to the organisation is going to be 0, vice versa the score is going to be 1.

Time orientation instead is a variable that takes under analysis the orientation of the risks described in the non-financial reports. In case the disclosure on the non-financial risks is backward oriented, so if risks refer to past events or to events occurring in the present, the score assigned to the company is going to be 0. In case the disclosure is forward oriented, so if disclosure of risks is oriented towards the future and considers events which may incur in a subsequent moment, the score to be assigned to the company is 1.

The choice of these two variables described above as tools to assess the qualitative aspects of non-financial risk disclosure, follows the theory proposed by Beattie, McInnes and Fearnley in 2004[99]; these authors proposed a methodology for analysing and assessing the disclosure on annual reports, and according to them each item of information has three type attributes based on: financial/non-financial nature of the information, backward/forward looking character and quantitative/non-quantitative aspect. Since this study focuses only on non-financial risks, the other two attributes have been chosen as discriminatory variables to evaluate the qualitative aspects of the non-financial risks disclosure of the pool of companies selected.

The third variable adopted refers to the tone of the report: whether the content is simply descriptive, hence neutral (the score derived from the dummy variable is going to be 1), whether the content has a negative tone, so if the communication of risks highlights the negative impacts of itself on the activities of the organisation (in this case the score is going to be 0) or f the content has a positive tone, so even though the company represents the concrete existence of a risk, its effects are perceived as an opportunity (the score assigned to the

[99] Beattie V., McInnes B. and Fearnley S., *A methodology for analysing and evaluating narratives in annual reports: a comprehensive descriptive profile and metrics for disclosure quality attributes,* Accounting Forum 28, pp. 205–236, 2004.

variable in this case is 2). This "tone" variable has been extracted from the paper of Caglio, Melloni and Perego, published in 2020 on the topic of content analysis and textual attributes of integrated reporting, in order to emphasize the positive or negative nature of the communication.[100]

The fourth discriminant implemented to describe the qualitative aspect of disclosure is a "volume" variable referring to the quantity of pages providing disclosure upon non-financial risks and how these are managed. The score of the variable is going to be the ratio between the number of pages in which the risks disclosed by the company at issue are described and the total number of pages of the report. This ratio is going t be expressed as a percentage, to show the amount of time and space dedicated to non-financial risk disclosure.

At the end of the qualitative analysis, each company will find itself we a score assigned for each variable and for each year of the triennium analyses. In order to simplify and summarise all of the evaluations, a comprehensive score defined as NFR (ql) will be assigned to each organisation and will be the algebraic sum of the first three variables described above. The fourth variable related to volume, will be considered as a descriptive assessment indicating the importance in terms of "space" reserved to non-financial risks disclosure.

At the end it will be interesting to verify if our hypothesis will be confirmed or not. In other words, the focus is going to be addressed towards the companies' performance, so if organisations implementing more sophisticated ERM systems and with a higher ERM score actually received a greater comprehensive score (and so disclose more information concerning the non-financial risks they have to manage) also relatively to non-financial risk disclosure (NFR score), which will be calculated as the sum between the NFR (qn) score and the NFR (ql) score.

[100] Caglio A., Melloni G. & Perego P., *Informational Content and Assurance of Textual Disclosures: Evidence on Integrated Reporting*, European Accounting Review, 29:1, 55-83, 2020.

5.4 Analysis of the results

Table 2 provides a synthesis of the elements taken under analysis to assess the level of ERM implementation in the organisations of the sample at issue. Along with the six criteria described above, also a small definition of the variables is provided.

Table 2 – Variable labels and definitions for ERM score

VARIABLES	DEFINITIONS
CRO	Dummy variable equal to 1 if the company has designed a chief risk officer or an ICR officer, and 0 otherwise
RISK COMMITTEE	Dummy variable equal to 1 if the company has designated a specific risk committee or an ICR committee, and 0 otherwise
RC TO BoD	Dummy variable equal to 1 if the CG body responsible for risk management, i.e., the specific risk committee or the ICR committee or, these two lacking, the IC committee, refers to the BoD at least biannually, and 0 otherwise
RA FREQUENCY	Dummy variable equal to 1 if the company performs the risk assessment procedure at least biannually, and 0 otherwise
RA LEVEL	Dummy variable equal to 1 if the company carries out the risk assessment procedure at a level lower than the overall company (e.g., by business unit or function), and 0 otherwise
RA METHOD	Dummy variable equal to 1 if the company adopts both qualitative and quantitative methods of risk assessment, and 0 otherwise
ERM SCORE	Sum of the following variables: CRO, RiskCommittee, RCtoBoD, RAfrequency, RAlevel, RAmethod
ERM ADVANCED	Dummy variable equal to 1 if ERMscore is equal to or higher than 4, and 0 otherwise

Source: Florio C. and Leoni G., *Enterprise risk management and firm performance: The Italian case*, The British Accounting Review, 49, p. 62, 2017.

The last two rows report respectively the computation system adopted to define the ERM score of each company and the methodology to determine whether the company is considered "advanced" or not, from an ERM approach.

Table 3 presents only the financial companies of the FTSE MIB index and gives a better view of how they perform in their ERM approach and whether their level of implementation is satisfactory enough. After the first skimming of companies according to the industry of belonging, whether their level of ERM systems are considered "advanced" or not, supports the choice of the organisations to include in the sample to analyse. The pool of "worst" companies is quite simple to create since there are only three companies, which performed poorly in terms of ERM system implementation. These companies, shaded in red, are Azimut Holding, Banco BPM and Exor. For what concerns the creation of the pool of "best", the choice is more difficult, since the remaining eleven companies present high scores, showing how their ERM systems are more sophisticated. As a first selection, companies that attained an ERM score equal to four have been excluded: this narrows the choice to eight companies presenting an ERM score of five. At this point, the final decision has been based on a preliminary revision of the corporate governance reports and sustainability and non-financial reports of the

companies in the following years, in order to select on both a quantitative and qualitative basis the ones with greater data available, hence the ones to include into the sample of "best" companies. The choice of the "best" ", shaded in green, includes: Finecobank, Intesa Sanpaolo and Ubi Banca.

Table 3 – ERM score of financial companies

FTSE MIB COMPANY	CORPORATE GOVERNANCE REPORT 2018								
	industry	CRO	Risk Committee	RC to BoD	RA frequency	RA level	RA Method	ERM score	ERM Advanced
Atlantia	Financial	1	1	1	0	1	0	4	1
Azimut Holding	Financial	1	1	0	0	1	0	3	0
Banca Generali	Financial	1	1	1	0	1	1	5	1
Banca Mediolanum	Financial	1	1	1	0	1	1	5	1
Banco BPM	Financial	0	1	1	0	1	0	3	0
Bper Banca	Financial	1	1	1	0	1	1	5	1
Exor	Financial	0	1	0	1	0	0	2	0
Finecobank	Financial	0	1	1	1	1	1	5	1
Generali	Financial	1	1	1	0	1	1	5	1
Intesa San Paolo	Financial	1	1	1	1	1	0	5	1
Mediobanca	Financial	1	1	1	1	1	0	5	1
Ubi Banca	Financial	1	1	1	1	1	0	5	1
Unicredit	Financial	1	1	0	1	1	0	4	1
Unipol	Financial	0	1	1	1	1	0	4	1

In order to give a better overview of the level of sophistication of the ERM systems of the companies selected for conducting the study, table 4 shows in greater detail the ERM score of the six companies for each year taken under analysis during this study. Also for the following years (2019 and 2020), the ERM score has been derived according to the criteria defined in the previous paragraph and used for the year 2018.

Table 4 – ERM score of "Best" and "Worst" sample

FTSE MIB COMPANY	CORPORATE GOVERNANCE REPORT 2018						
	CRO	RC	RC to BoD	RA FREQUENCY	RA LEVEL	RA METHOD	ERM-SCORE
FINECOBANK (BEST)	0	1	1	1	1	1	5
INTESA SANPAOLO (BEST)	1	1	1	1	1	0	5
UBI BANCA (BEST)	1	1	1	1	1	0	5
AZIMUT HOLDING (WORST)	1	1	0	0	1	0	3
BANCO BPM (WORST)	0	1	1	0	1	0	3
EXOR (WORST)	0	1	0	1	0	0	2

FTSE MIB COMPANY	CORPORATE GOVERNANCE REPORT 2019						
	CRO	RC	RC to BoD	RA FREQUENCY	RA LEVEL	RA METHOD	ERM-SCORE
FINECOBANK (BEST)	0	1	1	1	1	1	5
INTESA SANPAOLO (BEST)	1	1	1	1	1	0	5
UBI BANCA (BEST)	1	1	1	1	1	0	5
AZIMUT HOLDING (WORST)	1	1	0	0	1	0	3
BANCO BPM (WORST)	0	1	1	0	1	0	3
EXOR (WORST)	0	1	0	1	0	0	2

FTSE MIB COMPANY	CORPORATE GOVERNANCE REPORT 2020						
	CRO	RC	RC to BoD	RA FREQUENCY	RA LEVEL	RA METHOD	ERM-SCORE
FINECOBANK (BEST)	1	1	1	1	1	1	6
INTESA SANPAOLO (BEST)	1	1	1	1	1	0	5
UBI BANCA (BEST)	1	1	1	1	1	0	5
AZIMUT HOLDING (WORST)	0	1	0	0	1	1	3
BANCO BPM (WORST)	0	1	1	0	1	0	3
EXOR (WORST)	0	1	0	1	0	0	2

From the data extracted from the corporate governance report of each company, one observation should be highlighted. In year 2020 Finecobank increased its score from five to six, due to the appointment of a Chief Risk Officer (CRO) elected by the Board of Directors. In this sense, Finecobank has implemented an ERM approach and a series of activities that could be defined as extremely advanced and consistent, according to the assessment parameters chosen. The table also shows a change for Azimut Holding: not in terms of comprehensive ERM score, since it remains the same across the whole triennium, but in terms of individual score of the parameters. In fact, the corporate governance report of 2020 highlighted the absence of a CRO but in exchange it shows the presence of a risk assessment methodology, as

the COSO framework suggests. Hence, after an initial qualitative risk screening, Azimut Holding managers performed also a quantitative analysis on the most critical risks.

Since the sample of organisation to analyse has been defined and their ERM score has been provide, the focus is going to move towards the topic of non-financial risk disclosure. More specifically, all sustainability or non-financial statements of each company have been read and analysed in order to assess the level of disclosure from the perspective of non-financial risks. A premise is necessary: for the year 2018 Finecobank didn't provide any non-financial report in the "investor relations" area of the website, hence the lack of availability of such document subtracts the possibility to conduct this type of analysis for the first year of the timeframe at issue. For what concerns the rest of the companies, no further clarifications are necessary. Table 5 shows the information gathered in the sustainability reports the companies involved in the study as an expression of the quantitative aspects pointed out in the previous paragraph. For each organisation, the analysis consisted in observing the disclosure concerning the risks listed by the companies and verify whether these events refer to the fourteen elements cited into the EU 2014/95 Directive. The extracts taken from the non-financial report of each company are available in Appendix A at the end of the chapter, in order to show the explicit reference to the elements of the directive used as evaluation criteria inside the documents published.

Table 5 – NFR (qn) Score of "Best" and "Worst" sample

FTSE MIB COMPANY	QUANTITATIVE VARIABLES 2018														
	Impact	Energy	Gas	Water	Air	Gender	Dialog	Workers	Trade Union	HS	Local Community	Human Rights	Corruption	Bribery	NFR(qn) SCORE
FINECOBANK (BEST)	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
INTESA SANPAOLO (BEST)	1	1	1	0	0	1	1	1	0	1	1	1	1	1	11
UBI BANCA (BEST)	1	1	0	0	0	1	0	1	1	1	1	1	1	1	10
AZIMUT HOLDING (WORST)	1	0	0	0	0	1	1	0	0	1	0	0	1	0	5
BANCO BPM (WORST)	0	1	1	0	0	0	1	0	1	1	1	0	1	1	8
EXOR (WORST)	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1

FTSE MIB COMPANY	QUANTITATIVE VARIABLES 2019														
	Impact	Energy	Gas	Water	Air	Gender	Dialog	Workers	Trade Union	HS	Local Community	Human Rights	Corruption	Bribery	NFR(qn) SCORE
FINECOBANK (BEST)	1	1	1	0	0	1	1	1	1	1	0	1	1	1	11
INTESA SANPAOLO (BEST)	1	1	1	0	0	1	1	1	0	1	1	1	1	1	11
UBI BANCA (BEST)	1	1	1	0	0	1	0	1	1	1	1	1	1	1	11
AZIMUT HOLDING (WORST)	1	0	1	0	0	1	1	0	0	1	0	0	1	0	6
BANCO BPM (WORST)	0	1	1	0	0	0	1	1	0	1	1	0	1	1	8
EXOR (WORST)	0	0	0	0	0	0	0	0	0	0	0	0	1	1	2

FTSE MIB COMPANY	QUANTITATIVE VARIABLES 2020														
	Impact	Energy	Gas	Water	Air	Gender	Dialog	Workers	Trade Union	HS	Local Community	Human Rights	Corruption	Bribery	NFR(qn) SCORE
FINECOBANK (BEST)	1	1	1	0	0	1	1	1	1	1	0	1	1	1	11
INTESA SANPAOLO (BEST)	1	1	1	0	0	1	1	1	0	1	1	1	1	1	11
UBI BANCA (BEST)	1	1	1	0	0	1	0	1	1	1	1	1	1	1	11
AZIMUT HOLDING (WORST)	1	0	1	0	0	1	1	0	0	1	0	1	1	0	7
BANCO BPM (WORST)	0	1	1	0	0	0	1	1	0	1	1	0	1	1	8
EXOR (WORST)	0	0	0	0	0	0	0	0	0	0	0	0	1	1	2

As explained previously through the description of the methodology, each column refers to one of the fourteen elements reported in the European directive to be included in the non-financial disclosure for large companies; the final column shows a score for each company, defined as NFR (qn) score, in other words it is the sum of the single scores attained by the companies for each element, showing the level of non-financial risk disclosure from a quantitative perspective. The results show that there is an actual discrepancy between the best companies and the worst. In particular way, among the "best", Ubi Banca experiences an increase in its score from 2018 to 2019, due to the compliance concerning the disclosure of information referred to greenhouse gas (GHG) emissions and strategies to mitigate this risk. On the other hand, it can be noticed that companies belonging to the sample of "worst" attain quite low scores with respect to the other group. Exor is assigned the lowest score, which increases of one point from 2018 and 2019, remaining unchanged in 2020; this fact shows that the organisation does not judge relevant the disclosure of information regarding non-financial risks they face and how they decide to manage and mitigate these risks. The reason of such decision could be attributable to the threat of disclosing key information to the

market, hence competitors, or to the fact that non-financial risks actually have a minimum impact on the activities of Exor, so managers consider unnecessary disclosure of risks other than financial. Banco BPM, instead is the company among the "worst" which attained the highest score in terms of quantitative non-financial disclosure and remain constant across the three years. In fact, under this perspective, Banco BPM performance in terms of non-financial risk disclosure appears to be quite disconnected to its level of ERM system implementation; the company actually seems oriented towards to an enhanced disclosure of non-financial risks, as companies with a greater ERM score, even though its approach to ERM practices is not effectively developed. An interesting fact to notice is that the NFR (qn) score of Azimut Holding increases from year to year and moves from five to seven; in detail the organisation experienced such growth due to the communication of risks deriving from GHG emissions of the company and potential violation of human rights.

Given the interest of the research in evaluating the level of non-financial risk disclosure, since the quantitative aspect of the study has been discussed, now the attention addresses towards the qualitative aspect to determine the level of disclosure.

Table 6 shows further results emerging form the analysis of the non-financial reports of the six companies involved, in particular way it evaluates the level of disclosure according to four descriptive variables.

The first fact that can be noticed is the parameter "quantification", all companies received a zero according to the implementation of the dummy variable technique. This is an interesting fact, since it resumes the underlying concept that companies tend to avoid the disclosure of information concerning the quantification of non-financial risks, or maybe some organisations actually do not quantify non-financial risks and potential losses connected to them. Secondly, it can be observed that only companies with the best ERM scores actually disclose information on non-financial risks which are forward oriented and consider future events potentially harmful for the company in the long term. It must be drew attention to the fact that disclosure on risks considered forward-looking refers mainly to those risks related to environmental aspects. The companies analysed tend to inform stakeholders on how the activities of the company impact the environment, on the expectations of energy consumption in the future and consequences of the risk represented by the company's impacts; sustainability reports also communicate how these organisation plan to mitigate the effects of their operations on climate change, energy consumption and GHG emissions and confirm the efforts made to comply with the long-term European regulations and action plans to mitigate pollution and preserve the environment.

Table 6 - NFR (ql) Score of "Best" and "Worst" sample

FTSE MIB COMPANY	QUALITATIVE VARIABLES 2018				
	Quantification	Time Orientation	Tone	NFR (ql) SCORE	Volume
FINECOBANK (BEST)	-	-	-	-	-
INTESA SANPAOLO (BEST)	0	1	0	1	2,67%
UBI BANCA (BEST)	0	0	1	1	3,33%
AZIMUT HOLDING (WORST)	0	0	1	1	1,11%
BANCO BPM (WORST)	0	0	2	2	6,25%
EXOR (WORST)	0	0	0	0	0,89%

FTSE MIB COMPANY	QUALITATIVE VARIABLES 2019				
	Quantification	Time Orientation	Tone	NFR (ql) SCORE	Volume
FINECOBANK (BEST)	0	1	1	2	4,86%
INTESA SANPAOLO (BEST)	0	1	0	1	2,67%
UBI BANCA (BEST)	0	1	1	2	1,11%
AZIMUT HOLDING (WORST)	0	0	1	1	1,19%
BANCO BPM (WORST)	0	0	1	1	4,30%
EXOR (WORST)	0	0	0	0	0,84%

FTSE MIB COMPANY	QUALITATIVE VARIABLES 2020				
	Quantification	Time Orientation	Tone	NFR (ql) SCORE	Volume
FINECOBANK (BEST)	0	1	1	2	5,36%
INTESA SANPAOLO (BEST)	0	1	0	1	2,92%
UBI BANCA (BEST)	0	1	0	1	7,04%
AZIMUT HOLDING (WORST)	0	0	1	1	0,07%
BANCO BPM (WORST)	0	0	1	1	4,60%
EXOR (WORST)	0	0	0	0	0,09%

Another interesting aspect to underline in this table refers to the variable "tone": none of the companies involved in the study (neither the best ones nor the worst) presented a positive tone in the reports that have been analysed, they always showed themselves neutral in their disclosure of non-financial risks or negative, which means that communication regarding non-financial risks highlights the negative effects of them on the company. The only exception for what concerns the tone of the reports can be observed for Banco BPM in 2018: even though the ERM score is one of the lowest, this organisation is the only one which reported information on non-financial risks in its sustainability report through a positive tone, which means that besides the explanation of the risks faced by the company, the effects of these events are described as an opportunity for the organisation, not a simple threat. This idea recalls the concept expressed in chapter 1 of risk as a double-sided event and that contemporary risk management focuses on the upside risk of an event potentially affecting the company in the future.

As a final consideration, table 6 shows that the NFR (ql) score, which is the score attained by each company according to the evaluation of these qualitative variables referring to non-financial risk disclosure, is more or less homogeneous across the three years, with small changes. Also the presence of the "Volume" variable shows that the best companies from the ERM score perspective, present in their non-financial statements the greatest number of pages related to non-financial risks. This lets suppose that companies more engaged with ERM approaches and activities disclose more quantity of information (in terms of pages) on non-financial risks.

Given all the data relative to the level of implementation of ERM systems in each company of the sample, to the quantitative and qualitative analysis on non-financial risk disclosure, it is possible to draw an overall score of the non-financial variable, defined as the NFR score.

The NFR score is simply the algebraic sum of the NFR (qn) score and the NFR (ql) score for each firm taken under analysis.

$$\text{NFR SCORE} = \text{NFR (qn) SCORE} + \text{NFR (ql) SCORE}$$

Table 7 sums up the scores regarding the level of non-financial risk disclosure and shows for each organisation involved, the comprehensive score evaluating this aspect, in order to enable the comparison with the ERM score and verify the truthfulness of the initial hypothesis.

Table 7 – NFR SCORE of the sample

FTSE MIB COMPANY	NFR SCORE 2018		
	NFR (qn) Score	NFR (ql) Score	NFR SCORE
FINECOBANK (BEST)	-	-	-
INTESA SANPAOLO (BEST)	11	1	12
UBI BANCA (BEST)	10	1	11
AZIMUT HOLDING (WORST)	5	1	6
BANCO BPM (WORST)	8	2	10
EXOR (WORST)	1	0	1

FTSE MIB COMPANY	NFR SCORE 2019		
	NFR (qn) Score	NFR (ql) Score	NFR SCORE
FINECOBANK (BEST)	11	2	13
INTESA SANPAOLO (BEST)	11	1	12
UBI BANCA (BEST)	11	2	13
AZIMUT HOLDING (WORST)	6	1	7
BANCO BPM (WORST)	8	1	9
EXOR (WORST)	2	0	2

FTSE MIB COMPANY	NFR SCORE 2020		
	NFR (qn) Score	NFR (ql) Score	NFR SCORE
FINECOBANK (BEST)	11	2	13
INTESA SANPAOLO (BEST)	11	1	12
UBI BANCA (BEST)	11	1	12
AZIMUT HOLDING (WORST)	7	1	8
BANCO BPM (WORST)	8	1	9
EXOR (WORST)	2	0	2

As the table above shows, the final results obtained from the analysis of the corporate governance report and sustainability or non-financial report of each company answer to initial research question posed at the beginning of the chapter and confirm the initial hypothesis. Companies which implemented more sophisticated processes of ERM and more careful in the approach to activities related to risk management actually disclose to investors and stakeholders in general greater information, in terms of quantity and quality, concerning non-financial risks and their management.

5.5 Discussion

The empirical study conducted exploits the existing literature and research to evaluate both the level of implementation of ERM systems and the level of non-financial risk disclosure for a sample of companies listed in the Italian FTSE MIB index. The aim of this research was to investigate whether there is a relation between ERM and non-financial risk disclosure, more specifically, the initial hypothesis claims that companies which demonstrate to approach ERM systems and activities in a more integrated way and which developed more sophisticated processes actually increase the level of communication to stakeholders for what concerns the disclosure on risks related to non-financial aspects and issues.

During the revision and analysis of the non-financial reports of the companies involved in the study, an interesting fact can be noticed: all of the organisations tend to disclose more or less the same information on non-financial risks across the three years timeframe taken under consideration. The variation in disclosure and on the topics of the disclosure is minimal, in fact in many cases it is possible to observe a "copy and paste" situation of the sentences and information communicated, especially for the companies performing more poorly (the ones pertaining to the "worst" category according to the ERM score). This characteristic could imply the fact that non-financial disclosure, especially related to risks and their management, is still an excessively discretionary requirement, even though some regulations and directives have been provided. Whether to inform stakeholders thoroughly and in a detailed way upon non-financial issues such as risks is a decision based on the willingness of the organisation and on the advantages, in terms of relations with investors and reputation, perceived and evaluated by the board.

A curious outcome emerging from the results of the research involves Banco BPM. As it has been ascertained through the assessment of the ERM score and NFR score, this organisation, even though classified among the category with lower ERM scores, showed a tendency to move towards the performances observed in the "best" organisation. In particular way it is possible to verify this tendency from the quantitative perspective adopted to evaluate the level of non-financial risk disclosure. As showed by the data, BPM performs significantly better than the other two organisations in its category, however not enough to be included between the best ones. It has been possible to verify this fact also in terms of tone of the non-financial reports: as underlined above, Banco BPM is the only company that attained a maximum score for that variable in 2018. However, the most meaningful data concerning the evaluation of non-financial risk disclosure consists in the "volume" variable: BPM is the company with one of the highest percentages. Of course, part of this result may be

attributable to the length of reports (even though only Intesa Sanpaolo published in the three years reports consistently longer than the ones on BPM, Finecobank and Ubi published documents more or less the same length as the ones of BPM), however this fact confirms the trend of Banco BPM in improving its level and quality of disclosure across time.

The analysis conducted on ERM systems implemented by the organisation under investigation and on the non-financial information disclosed in the past reports essentially confirmed the expectations and the hypothesis conceived at the beginning: organisations which received a higher ERM score, also attained higher scores for what concerns the level of non-financial risk disclosure. This finding is very interesting because it supports the idea of a relationship existing between management and disclosure, in more detail between the quality of risk management and the amount of information concerning non-financial risks, which companies are willing to disclose to their stakeholders.

As a matter of fact, the results emerged from this empirical study support two of the theories presented in paragraph 4.5 regarding voluntary disclosure: signalling and agency theory. The research investigated upon the levels of non-financial risk disclosure and the outcome confirmed the fact that companies implementing more advanced systems of ERM actually disclose a higher level of information of non-financial risks. Hence, the relation with voluntary disclosure is consequential, because besides the establishment of some directives, non-financial disclosure still relies a lot on the willingness of companies and their attitude towards a more detailed provision of data.

In this sense, the research supports the signalling theory because the analysis of the results showed that organisations performing better from a risk management perspective and showing greater ability in implementing ERM systems, in concrete disclose more relevant information on non-financial risks than others, in terms of quantity and quality. This may be the result of an interest by the best companies to provide additional information (with respect to minimum requirements) to stakeholders and investors, "signalling" to the market the fact that their level of disclosure is higher and more consistent. In particular way, more detailed disclosure on risks faced by the company and on the way these risks are managed contributes to enhance the entity's reputation and may increase the value of stocks in the market. Also the agency theory is supported by this study, since the greater level of implementation of ERM systems and a more developed culture corresponds to higher level of disclosure by organisations. Probably, enhancing the monitoring activity over the entity's operations and managers' conduct, favoured the supervision of the board over the enterprise and ensured a more consistent flow of information regarding non-financial risks. As a result, managers

(agents), in order to increase their accountability and reduce information asymmetry, could be more incline in providing into reports more information than required.

Conclusions

This research deals with the topic of risk management and non-financial risk disclosure to stakeholders. More specifically, the composition follows a logical order to link these two main subjects, creating a path from the presentation of ERM and the frameworks created to enhance the adoption and implementation of such approach, through the importance of managing non-financial risks up to the topic of disclosure and its evolution, stressing the relevance of communicating with stakeholders and the strategic decision behind voluntary disclosure. The paper ends with an empirical study conducted on a sample of Italian companies, trying to highlight a possible connection between ERM processes and non-financial risk disclosure.

As illustrated in chapter one, risk management faced various steps in its evolution from traditional risk management concerned with hedging the organisation from pure risks to enterprise risk management: a business culture embracing an holistic approach towards risk management and favouring integrated system of managing risk through the interaction with business strategy and value creation process, in order to exploit the upside risk of events and turn a potential threat into an opportunity of growth. The adoption of ERM for organisations has been facilitated by the existence of various frameworks, above all the one proposed by COSO in 2004 and revised in 2017. This framework allows organisations to understand the value underlying in ERM and favours the implementation of such approach due to detailed descriptions of actions to undertake and a clear vision to embrace.

Also the topic of disclosure experienced a deep change across years, due to the pressure exercised by regulation, which imposes an increasingly clear and explicit disclosure, not only regarding financial performance or results obtained, but also regarding themes related to the environmental impact and long-term sustainability of organisations. In fact, large companies are obliged to disclose a specific non-financial report upon these topics and also other companies are encouraged by regulators to follow this model. In particular way, chapters three and four tackle and stress the relevance of non-financial risks in terms of direct impact on performance and indirect ones, especially for what concerns the relation with stakeholders and potential investors. On this issue the importance of voluntary disclosure and the theories underlying this approach have been discussed: the fact that a company decides to disclose on a voluntary basis more information than the one required by regulations can have a positive impact on the reputation of the company, but most importantly gives the possibility to

investors to evaluate with greater precision the situation of the company, hence whether to invest or not.

The paper concludes with an empirical study on listed companies in Italy, which actually demonstrates a relationship between ERM and non-financial risk disclosure, in fact companies with a more consistent ERM culture revealed also more effective in the communication of non-financial risks to their stakeholders, from both a quantitative and qualitative point of view. However the study emerged a tendency of organisations to focus on non-financial risks currently threatening the company, with very little communication of future perspectives. Only in the case on environmental issues, companies disclosed information on risks referred to long term situations and mitigation processes, generally coinciding with the European objectives; for what concerns non-financial threats other than environmental almost no information have been disclosed.

Furthermore, also the aspect of a quantitative evaluation of risks and the tone of the report could be subject of investigation for future studies. From this research it emerged that companies do not quantify non-financial risks, or at least they do not disclose any information concerning this characteristics. The lack of a quantification of non-financial risks may influence negatively the assessments of investors but also the revision processes and self-evaluations made by the organisation itself. Associating numbers and figures to a qualitative description of risks incurred by the company may enhance the mitigation processes and favour a more efficient decision-making process to manage these risks; furthermore it would confer more consistency and reliability to information provided to stakeholders, making the entire communication more complete. Also the tone of non-financial reports is an aspect that could be investigated by further research. This study drew attention to the fact that the organisations involved in the study mostly disclosed their information through a neutral communication system, limiting their considerations to a descriptive analysis. In this way, the communication results generic and in some cases it is difficult to deduct the attitude towards the risk discussed. This choice of neutral positioning doesn't allow the organisation to communicate eventual opportunities emerging from risks, which is in contrast with one of the main concepts of ERM culture. The fact of withstanding passively the effects of a risky event doesn't create any opportunity for the organisation, on the other hand an active and propositional approach towards risks allows the evaluation of potential growth opportunities that, instead of harming the operations of the company, could create new situations to exploit and generate value for all stakeholders.

In this sense it is clear that ERM and non-financial risk disclosure are correlated, however non-financial risk disclosure still has a longer development process in front of it, in order to reach the same attitude of integration and holistic vision proposed by ERM.

In relation to this final consideration, it is important to drive to the attention the European proposal discussed the twenty-first of April 2021, for a revision and in depth analysis of the contents of the EU 2014/95 "Non-financial reporting directive" (NFRD). More specifically, with this proposal the EU Parliament and Council underlined the issue concerning the fact that the non-financial information reported by companies does not meet the users' needs; there isn't enough comparability, reliability or accessibility to this kind of information, moreover there is an excessive multitude of overlapping reporting standards and frameworks generating confusion on what type of information companies should actually report. For this reason, the proposal of a "Corporate Sustainability Reporting Directive" (CSRD) aims to ensure that companies from whom users need non-financial information report such information, and that reported information is relevant, comparable, reliable, and easy to access and use. It also aims to reduce unnecessary costs for preparers by providing detailed guidelines on what information shall be reported. As a consequence, investors will be able to better evaluate the sustainability risks and impacts of investments, which translates into mobilisation of private finance in support of the European Green Deal and reinforcement of the social contract between companies and society, by making companies more accountable for their impact on the community and the environment.

As a matter of fact, the European Union is concretely working towards the creation of a standard and framework of reference to help both organisations and stakeholders: the first ones in the disclosure of non-financial information and in the assurance process, the others under the perspective of the provision of reliable and comparable documents to carry out more precise and effective evaluations. Not least, the importance of such proposal reflects also on society, because besides the positive externalities for the world of business and the market, also the community and civil society is going to gain advantage from a more diligent and careful management of non-financial issues. This future perspective for non-financial disclosure, actually blends perfectly with the holistic approach and vision proposed by the culture embedded in ERM and supports the idea that modern risk management must face financial and non-financial events through an integrated approach, which involves strategy, vision, mission and all business units of the organisation, because all of these elements are interrelated among each other and all together participate to the value generation process of the enterprise.

Appendix A

BEST COMPANIES	REPORT YEAR 2018	NFR SCORE
FINECO BANK		-
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
		NFR SCORE
INTESA SANPAOLO		11
1	Changes in environmental regulations and standards that the Group voluntarily adheres to (ISO standards) (p.51) - **FL**	
2	Changes in the regulations and incentives on renewable energy (p.53) - **FL**	
3	Introduction of new greenhouse gas emission limits or new related reporting systems Increased cost of greenhouse gas emissions (p.51) - **FL**	
4		
5		
6	Insufficient focus on diversity and inclusion issues (p.47)	
7	Employment law risks (p.36)	
8	Conflicts and related labour dispute risks (p.47)- **FL**	
9		
10	Health and safety of employees (p.47)	
11	social and economic development of local communities (p.36)	
12	the analysis of potential risk areas in the sphere of human rights which, for every principle in the international conventions, outlines the possible impacts of the company's operations on its stakeholders and the relative company regulations (p.153)	
13	Risks of non-compliance with applicable legislation (corruption, money laundering, taxation, free competition, privacy, labour law) and ineffective response to regulatory changes (p.46)	
14	Cfr. 13	
		NFR SCORE
UBI BANCA		10
1	Natural disasters, extreme weather events and other consequences of climate change. (p.22)	
2	Inefficient management of energy and other nonrenewable natural resources (p.22)	
3		
4		
5		
6	Incidents relating to nondiscrimination and occupational health and safety. (p.21)	
7		
8	Tensions and/or unrest (p.21)	
9	Cfr 8	
10	Incidents relating to nondiscrimination and occupational health and safety. (p.21)	
11	Unemployment or underemployment, crisis in the welfare system, increased poverty and inequality. (p.22)	
12	non-compliance risks and actively managing reputational risk, with reference to human rights (p.18)	
13	Cfr. 14	
14	Involvement in activities and practices that are illegal/controversial from an ethical, environmental or social viewpoint. (p.20)	

WORST COMPANIES	REPORT YEAR 2018	NFR SCORE
AZIMUT		5
1	the impact of the Group's operations is considered in terms of paper consumption (p.72)	
2		
3		
4		
5		
6	• Employees' hiring and termination (p.58)	
7	the Group identified some potential risks related to personnel relationships. Specifically: • Employees' hiring and termination • Remuneration • Wrong selection of resources (p.58)	
8		
9		
10	The risks related to health and safety are analysed in accordance with the applicable ruling legislation. (p.58)	
11		
12		
13	The Group's current risk management system identifies the corruption risks mainly related to possible instances of active corruption. (p.58)	
14		
		NFR SCORE
BANCO BPM		8
1		
2	USE OF NON-RENEWABLE NATURAL RESOURCES, ENERGY INEFFICIENCY AND FAILURE TO RECYCLE (p.73)	
3	Cfr. 2	
4		
5		
6		
7	UNSUITABLE PROFESSIONAL PROFILES AND LOSS OF KEY RESOURCES (p.55)	
8		
9	CONFLICTS BETWEEN SOCIAL PARTNERS (p.57)	
10	HEALTH AND SAFETY (PHYSICAL AND PSYCHOLOGICAL) (p.55)	
11	REPUTATION AND UNRELIABLE COUNTERPARTIES (p.65)	
12		
13	CONFLICTS OF INTEREST AND CORRUPTION (p.65)	
14	Cfr. 13	
		NFR SCORE
EXOR		1
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13	The Group is also subject to risks inherent to operating globally, including compliance with applicable anti-corruption laws (p.131)	
14		

BEST COMPANIES	REPORT YEAR 2019	NFR SCORE
FINECO BANK		11
1	Natural disasters and public safety: Events caused by natural disasters or similar events. These events, in addition to having an impact in terms of operational losses, may have a social impact if the continuity of the business cannot be guaranteed (p.34)	
2	Risk of inadequate monitoring of the use of resources and energy consumption at Group level, with the consequent lack of measurable objectives in this area (p.34) - **FL**	
3	Risk of lack of adequate tools and methodologies to analyse the impact generated and sustained by the Group in the field of climate change and the evolution of legislation on the subject (p.34)	
4		
5		
6	Lack of effectiveness of programmes and initiatives related to diversity and equal opportunities (p.33) - **FL**	
7	Fall in employee engagement level with consequent impact on performance (p.33)	
8	Risk of human rights violations resulting from discriminatory behaviour in the company (p.34)	
9	Failure to comply with level-one legislation: (e.g. provisions of the Workers' Statute concerning the exercise of trade union rights) (p.34)	
10	Practices that do not comply with occupational health and safety laws or conventions, resulting in losses and harm to reputation (p.32)	
11		
12	Financing of and investment in unethical activities, activities that do not comply with standards and practices relating to Human Rights, working conditions and the environment. (p.32) - **FL**	
13	Risk of losses and harm to reputation due to the Group's involvement in both active and passive corruption. The risk relates not only to completed actions, but also to attempts, instigations and being an accessory (p.35)	
14	Risk of money laundering or funding terrorism: providing direct or indirect support for money laundering or funding terrorism. The risk has reputational consequences and also carries significant sanctions (p.35)	
INTESA SANPAOLO		NFR SCORE 11
1	Changes in environmental regulations and standards that the Group voluntarily adheres to (ISO standards) (p.49) - **FL**	
2	Changes in the regulations and incentives on renewable energy (p.48) - **FL**	
3	Changes in environmental regulations Introduction of new greenhouse gas emission limits or new related reporting systems (p.48) - **FL**	
4		
5		
6	Insufficient focus on diversity and inclusion issues (p.43)	
7	Employment and Labour law risks (p.32)	
8	Conflicts and related labour dispute risks (p.43)	
9		
10	Health and safety of employees (p.43)	
11	Bank's leadership in society for the dissemination of the sustainability culture Promotion and measurement of activities with high social impact (p.32)	
12	Aware that its activities have direct and indirect impacts on human rights, Intesa Sanpaolo has defined its areas of responsibility for each of its stakeholders (p.146)	
13	Risks of non-compliance with applicable legislation (corruption, money laundering, taxation, free competition, privacy, labour law) and ineffective response to regulatory changes (p.42)	
14	Cfr. 13	
UBI BANCA		NFR SCORE 11
1	Physical risks associated with climate change and natural and man-made disasters (p.22)	
2	Scarcity of resources for energy transition (p.22) - **FL**	
3	Transition risks associated with climate change (environmental regulations/standards, emissions limits, incentives, energy costs and raw materials) (p.22)	
4		
5		
6	Inadequate diversity management (p.21)	
7		
8	Involvement in activities and practices that are illegal/ controversial from an ethical, environmental or social viewpoint (p.20)	
9	Conflict with trade unions (p.21)	
10	Shortcomings in occupational health and safety management (p.21)	
11	Risks related to the social context (unemployment, underemployment, social instability, crises in the welfare system, increased poverty and inequality) (p.22)	
12	Protection of human rights - risk of conflict of interests (p.20)	
13	Risks relating to the business environment (illegal activities such as money-laundering, tax evasion and counterfeiting) (p.22)	
14	Involvement in activities and practices that are illegal/ controversial from an ethical, environmental or social viewpoint (p.20)	

WORST COMPANIES	REPORT YEAR 2019	NFR SCORE
AZIMUT		6
1	For the purposes of this document, the impact of the Group's operations is essentially considered in terms of paper consumption and electricity used.(p.78)	
2		
3	Cfr. 1	
4		
5		
6	Employees' hiring and termination (p.60)	
7	the Group identified some potential risks related to personnel relationships. Specifically: • Employees' hiring and termination • Remuneration • Wrong selection of resources (p.60)	
8		
9		
10	The risks related to health and safety are analysed in accordance with the applicable ruling legislation. (p.60)	
11		
12		
13	The Group's current risk management system identifies the corruption risks mainly related to possible instances of active corruption. (p.60)	
14		
		NFR SCORE
BANCO BPM		8
1		
2	USE OF NON-RENEWABLE NATURAL RESOURCES, ENERGY INEFFICIENCY AND FAILURE TO RECYCLE (p. 92)	
3	Cfr. 2	
4		
5		
6		
7	LABOUR LAW (p. 77)	
8	CONFLICT AND RESISTANCE TO CHANGE (p.62)	
9		
10	HEALTH AND SAFETY (PHYSICAL AND PSYCHOLOGICAL) (p.64)	
11	UNRELIABLE COUNTERPARTY (p.77)	
12		
13	CONFLICTS OF INTEREST AND CORRUPTION (p.73)	
14	Cfr. 13	
		NFR SCORE
EXOR		2
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13	A violation of anti-bribery and anti-corruption laws is a serious offense for both companies and individuals, which can result in significant fines, reputational damage and imprisonment of individuals. (p.113)	
14	Cfr. 13	

BEST COMPANIES	REPORT YEAR 2020	NFR SCORE
FINECO BANK		11
1	Natural disasters and public safety: Events caused by natural disasters or similar events. These events, in addition to having an impact in terms of operational losses, may have a social impact if the continuity of the business cannot be guaranteed (p.48)	
2	Risk of inadequate monitoring of the use of resources and energy consumption at Group level, with the consequent lack of measurable objectives in this area. (p.48) - **FL**	
3	Risk of lack of adequate tools and methodologies to analyse the impact generated and sustained by the Group in the field of climate change and the evolution of legislation on the subject (p.48)	
4		
5		
6	Lack of effectiveness of programmes and initiatives related to diversity and equal opportunities. (p.47)	
7		
8	Fall in employee engagement level with consequent impact on performance (p.47)	
9	Failure to comply with level-one legislation: (e.g. provisions of the Workers' Statute concerning the exercise of trade union rights) p.48	
10	Practices that do not comply with occupational health and safety laws or conventions, resulting in losses and harm to reputation. (p.46)	
11		
12	Financing of and investment in unethical activities, activities that do not comply with standards and practices relating to Human Rights, working conditions and the environment (p.46)	
13	Risk of losses and harm to reputation due to the Group's involvement in both active and passive corruption. The risk relates not only to completed actions, but also to attempts, instigations and being an accessory (p.49)	
14	Risk of money laundering or funding terrorism: providing direct or indirect support for money laundering or funding terrorism. The risk has reputational consequences and also carries significant sanctions (p.49)	
		NFR SCORE
INTESA SANPAOLO		11
1	Operational protection in risk situations • Impact on costs and business investments • Risks related to climate change (p. 51)	
2	Increase or reduction in average temperatures. Increase in the use of renewable energy sources (p.74)	
3	Changes in environmental regulations Introduction of new greenhouse gas emission limits or new related reporting systems (p.72)	
4		
5		
6	• Diversity & inclusion managemen (p.50)	
7	Labour law risks (p.51)	
8	Conflicts and related labour dispute risks (p.64) Continuity of employment/Welfare, well-being and social safety nets (p.51)	
9		
10	Health and safety of employees (p.64)	
11	Promotion and measurement of activities with high social impact (p.51)	
12	Aware that its activities have direct and indirect impacts on human rights, Intesa Sanpaolo has defined its areas of responsibility for each of its stakeholders (p.192)	
13	• Corruption prevention (p.50)	
14	Fighting against corruption and combating money laundering (p.76)	
		NFR SCORE
UBI BANCA		11
1	Rischi correlati al degrado ambientale e alla disponibilità di risorse naturali (p.8)	
2	Rischi "di transizione" Politiche e legali (p.9)	
3	Rischi "di transizione" Politiche e legali (p.9)	
4		
5		
6	Inadeguata attenzione a diversità e inclusione (p.8)	
7		
8	Conflittualità e relativi rischi giuslavoristici (p.7)	
9	Cfr. 8	
10	Carenze nella gestione della salute e sicurezza sul lavoro (p.8)	
11	Rischi reputazionali correlati a finanziamenti in settori o operazioni controverse Scarsa attenzione ai temi sociali rilevanti nelle politiche commerciali e inadeguata selezione degli interventi di filantropia strategica (p.7)	
12	l'ambito operativo in cui vi può essere il rischio di violazione dei diritti umani appare limitato ai rischi correlati alle attività della clientela operante in alcuni settori economici (c.d. settori controversi, in particolare armi) e ai rischi derivanti dall'approvvigionamento di oro fisico. In considerazione del permanere di un volume di impieghi marginale, UBI Banca non ha adottato politiche specifiche nei confronti dei settori controversi, salvo che per quelli delle armi, per il quale è in essere una specifica Policy, e del gioco d'azzardo e scommesse, per il quale è in essere dal 2011 una direttiva interna dell'Area crediti. (p.16)	
13	Rischi reputazionali per coinvolgimento in attività e pratiche illegali/controverse dal punto di vista etico, ambientale o social (p.6)	
14	Rischi reputazionali per coinvolgimento in attività e pratiche illegali/controverse dal punto di vista etico, ambientale o social (p.6)	

WORST COMPANIES	REPORT YEAR 2020	NFR SCORE
AZIMUT		7
1	riconoscono il rischio legato agli impatti ambientali diretti derivanti dalle sedi (ad esempio monitoraggio emissioni, gestione rifiuti) p.73	
2		
3	riconoscono il rischio legato agli impatti ambientali diretti derivanti dalle sedi (ad esempio monitoraggio emissioni, gestione rifiuti) p.73	
4		
5		
6	identificano il tema del rischio di violazione dei diritti umani nell'ambito della gestione del personale, in termini di rischio di possibili discriminazioni (p.73) (non viene citata esplicitamente la parità di genere, tuttavia ho ritenuto di considerare tale questione racchiusa nel termine "discriminazioni"	
7		
8		
9		
10	i rischi attinenti alla salute e sicurezza sono analizzati con le modalità previste dalla normativa vigente in materia nei singoli paesi (p.72)	
11		
12	identificano il tema del rischio di violazione dei diritti umani nell'ambito della gestione del personale, in termini di rischio di possibili discriminazioni (p.73)	
13	Gli attuli sistemi di valutazione del rischio delle singole società contrllate dal gruppo individuano rischi connessi alla corruzione principalmente afferenti alla possibilità che si verifichino episodi di corruzione attiva (p.72)	
14		
BANCO BPM		NFR SCORE 8
1		
2	USE OF NON-RENEWABLE NATURAL RESOURCES, ENERGY INEFFICIENCY AND FAILURE TO RECYCLE (p.103)	
3	USE OF NON-RENEWABLE NATURAL RESOURCES, ENERGY INEFFICIENCY AND FAILURE TO RECYCLE (p.103)	
4		
5		
6		
7	NON-COMPLIANCE WITH LEGISLATIVE AND REGULATORY PROVISIONS (p.93)	
8	CONFLICT AND RESISTANCE TO CHANGE (p.69)	
9		
10	HEALTH AND SAFETY (PHYSICAL AND PSYCHOLOGICAL) (p.75)	
11	REPUTATIONAL DAMAGE, UNRELIABLE COUNTERPARTY, CONFLICTS OF INTEREST AND CORRUPTION - the support of progress and the wellbeing of the local area.(p.85)	
12		
13	REPUTATIONAL DAMAGE, UNRELIABLE COUNTERPARTY, CONFLICTS OF INTEREST AND CORRUPTION (p.85)	
14	COMPLIANCE (anti-money laundering controls) (p.88)	
EXOR		NFR SCORE 2
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13	A violation of anti-bribery and anti-corruption laws is a serious offense for both companies and individuals, which can result in significant fines, reputational damage and imprisonment of individuals. (p.125)	
14	Cf.r 13	

Bibliography

AA1000 Stakeholder Engagement Standard, AccountAbility, pp. 19-32, 2018.

Abraham S. & Shrives P. J., *Improving the relevance of risk factor disclosure in corporate annual reports*, The British Accounting Review, 46(1), pp. 91-107, 2014.

Bahar Gidwani, *The link between Sustainability and Brand Value*, in Thomas Singer (Ed.), Sustainability Matters, Research Report, R-1538-14-RR, p. 25, 2014.

Beattie V., McInnes B. and Fearnley S., *A methodology for analysing and evaluating narratives in annual reports: a comprehensive descriptive profile and metrics for disclosure quality attributes,* Accounting Forum 28, pp. 205–236, 2004.

Beck C., Dumay J., Frost G., *In Pursuit of a "Single Source of Truth": from Threatened Legitimacy to Integrated Reporting*, Journal of Business Ethics, 141(1), pp. 191-205, 2017.

Borsa Italiana, *Codice di Autodisciplina*, art. 7,P.1, 2011.

Borsa L., Frank, P., Doran, H., *"How can resilience prepare companies for environmental and social change?"*, Resilience: a journal of strategy and risk, Retrieved from PwC: https://www.pwc.com/gx/en/governance-risk-compliance-consulting-services/resilience/publications/pdfs/resilience-social.pdf.

Botosan C., *Disclosure level and cost of equity capital*, The Accounting Review, 72, 3, pp.323-345, 1997.

Brown Flynn and Society for Corporate Governance, *ESG Roadmap: Observations and Practical Advice for Boards, Corporate Secretaries and Governance Professionals,* p. 6, June 2018.

Caglio A., Melloni G. & Perego P., *Informational Content and Assurance of Textual Disclosures: Evidence on Integrated Reporting*, European Accounting Review, 29:1, pp. 55-83, 2020.

Cahan S. et al., *Are CSR disclosures value relevant? Cross-country evidence*, European Accounting Review, 25(3), pp. 579-611, 2016.

Campbell J. L., Chen H., Dhaliwal D. S., Lu H. & Steele L. B., *The information content of mandatory risk factor disclosure in corporate filings*, Review of Accounting Studies, 19(1), pp. 396-455, 2014.

Carroll A.B., Buchholtz A. K., Business & Society: Ethics, Sustainability, and Stakeholder Management, 8th edition, Cincinnati, OH: South-Western Cengage Learning, 2012.

Chapman R. J., *"Simple tools and techniques for Enterprise Risk Management",* John Wiley & Sons, 2006.

Chesley D., *The top changes to the COSO ERM Framework you need to know now* , Global, (APA) Risk Consulting Leader in PWC, 2017.

Citation by Microsoft's Jean-Francois Heitz, taken from *Enterprise-Wide Risk Management: strategies for linking risk and opportunity,* James W. Deloach, 2000.

COSO and WBCSD, *Enterprise Risk Management-Applying enterprise risk management to environmental, social and governance-related risks,* pp.40-41, October 2018.

COSO, "Enterprise Risk Management: executive summary", p. 2-8, www.coso.org, 2004.

COSO, *Enterprise Risk Management Integrating with Strategy and Performance,* Frequently Asked Question Section, pp. 5-8, 2017.

COSO, *Enterprise Risk Management: aligning risk with strategy and performance,* pp.53-54, June 2017 edition.

COSO, *Enterprise Risk Management: Integrating with Strategy and Performance,* p. 79, June 2017.

Crouhy M., D. Galai, R. Mark, *The essentials of risk management,* McGraw-Hill, p.15, 2006.

Damodaran, A., & Roggi, O., *Elementi di finanza aziendale e risk management. La gestione d'impresa tra valore e rischio*. Maggioli Editore, 2016.

Deegan C., Gordon B., *A study of the environmental disclosure practices of Australian corporations*, Account. Bus. Res., 26, pp. 187–199, 1996.

Deloach J., *Enterprise-Wide Risk Management: strategies for linking risk and opportunity*, p.23, 2000.

Dhaliwal D.S. et al., *Nonfinancial disclosure and analyst forecast accuracy: International evidence on corporate social responsibility disclosure*, Accounting Review, 87(3), pp. 723-759, 2012.

Dicuonzo G., *La disclosure sui rischi finanziari tra dottrina, normativa e prassi, Evidenze empiriche dal contesto italiano*, p.49, G. Giappichelli Editore, Torino, 2018.

Dobler M., *How Informative is Risk reporting? A Review of Disclosure Models*, Munich Business Research, Working Paper, n. 1, 2005.

Eiteman, D. K., Stonehill, A. I., & Moffett, M. H., Multinational business finance. Pearson Global Ed., 2016.

Elshandidy T. & Neri L., *Corporate governance, risk reporting practices, and market liquidity: Comparative evidence from the UK and Italy*, Corporate Governance: An International Review, 23(4), pp. 331-356, 2015.
Fink L., *Larry Fink's Annual Letter to CEOs: A Sense of Purpose.,* retrieved from BlackRock, 2018.

Floreani A., Enterprise Risk Management. I rischi aziendali e il processo di risk management, Pubblicazioni dell'I.S.U. Università Cattolica, Milano, 2004.

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

Flower J., *The international integrated reporting council: A story of failure*, Crit. Perspect. Account, 27, pp. 1–17, 2015.

Forestieri G., Risk management. Strumenti e politiche per la gestione dei rischi puri dell'impresa, Egea, 1996.

Gao F. Et al., *Determinants and Economic Consequences of Non-financial Disclosure Quality,* European Accounting Review. Taylor & Francis, 25(2), pp. 287-317, 2016.

Gobbi U., *L'assicurazione in generale*, Hoepli, Milano, 1898.

Global Reporting Initiative (GRI), Sustainability Reporting Guidelines G3, p.3, 2006.

Guthrie J., Parker L.D., *Corporate social reporting: A rebuttal of legitimacy theory.* Account. Bus. Res., 19, pp. 343–352, 1989.

Guthrie J., Petty R., Ricceri F., *The voluntary reporting of intellectual capital: Comparing evidence fromHong Kong and Australia*, J. Intellect. Cap., Vol. 7, pp. 254–271, 2006.

Hahn R. and Kuhnen M., *Determinants of sustainability reporting: a review of results, trends, theory, andopportunities in an expanding field of research*, Journal of cleaner production, 59, pp. 5-21, 2013.

International Integrated Reporting Council, IR Framework, p.10, 2021.

Iyer, S. R., Rogers, D. A., Simkins, B. J., & Fraser, J., *Academic research on enterprise risk management,* Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives (The Robert W. Kolb series in Finance), John Wiley & Sons, Inc., Hoboken, NJ, pp., 419-439, 2010.

John J. Hampton, *Fundamentals of Enterprise Risk Management: How Top Companies Assess Risk, Manage Exposure, and Seize Opportunity,* American Management Association AMACOM, 2009.

Kaiser T., *Managing non-financial risks: A new focus area for executive and non-executive board members,* Journal of risk management in financial institutions, 2015.

Kaplan R. S., *Accounting scholarship that advances professional knowledge and practice*, The Accounting Review, 86(2), pp. 367-383, 2011.

Khan, Mozaffar N., George Serafeim, and Aaron Yoon. *Corporate Sustainability: First Evidence on Materiality*, Harvard Business School Working Paper, No. 15-073, p.20, March 2015.

Kloman, H. F., *Enterprise Risk Management*, Chapter 2: A Brief History of Risk Management, p.19 – 29, 2011.
KPMG Advisory, Enterprise Risk Management in Italy, 2012.

KPMG, *The KPMG Survey of Corporate Responsibility Reporting*, p. 12, 2013.

Kravet T. & Muslu V., *Textual risk disclosures and investors' risk perceptions*, Review of Accounting Studies, 18(4), pp. 1088-1122, 2013.

La gestione del rischio aziendale, ERM – Enterprise Risk Management: modello di riferimento e alcune tecniche applicative, Associazione Italiana Internal Auditors (AIIA), PricewaterhouseCoopers (PwC), Committe of Sponsoring Organizations Treadway Commission (CoSo), Il Sole 24 Ore, 2006.

Lang M. and Lundholm R., *Corporate disclosure policy and analyst behaviour,* The Accounting Review, 71, pp.467-490, 1996.

Liebenberg A. P., Hoyt R. E., *"The determinants of Enterprise Risk Management: evidence from the appointment of chief risk officers"*, Risk Management and Insurance Review, Vol. 6, No. 1, pp. 37-52, 2003.

Lucian A. Bebchuk, Martijn Cremers, and Urs Peyer, *CEO Centrality*, NBER Working Paper n.13701, December 2007.

Martinez-FerreroJ., Ruiz-Cano D., Garcia-Sanchez I.M., *The Causal Link between Sustainable Disclosure and Information Asymmetry: The Moderating Role of the Stakeholder Protection Context*, Corporate Social Responsibility and Environmental Management, 23(5), pp. 319-332, 2016.

Metzger, E., Putt del Pino, S., Prowitt, S., Goodward, J., Perera, A., *SWOT: A Sustainability SWOT.* Retrieved from World Resources Institute: http://pdf.wri.org/sustainability_swot_user_guide.pdf.

Miihkinen A., *What Drives Quality of Firm Risk Disclosure? The Impact of a National Disclosure Standard and Reporting Incentives under IFRS*, in "The International Journal of Accounting", vol. 47, n. 4, pp. 437-468, 2012.
Milne M.J. and Gray R., *W(h)ither ecology? The triple bottom line, the global reporting initiative, and corporate sustainability reporting*, J. Bus. Ethics, 118, p. 20, 2013.

Mio C, Fasan M, Marcon C, Panfilo S., *Carrot or stick? An empirical analysis of the different implementation strategies of the EU directive on nonfinancial information across Europe*, Corporate Social Responsibility and Environmental Management, pp. 1–15, 2021.

Mitchell R. K., Van Buren H. J., Greenwood M., Freeman, R. E., Stakeholder Inclusion and Accounting for Stakeholders, Journal of Management Studies, Vol. 52 Issue7, pp. 851–877, 2015.

Moneva J. and Cuellar B., *The Value Relevance of Financial and Non-Financial Environmental*

Reporting, Environment Resource Economics 44, pp. 441–456, 2009.

Nolan J., *Corporate Accountability and Triple Bottom Line Reporting: Determining the Material Issues for Disclosure,* In Enhancing Corporate Accountability: Prospects and Challenges Conference Proceedings; University of New South Wales: Kensington, Australia, 2007.

Panfilo S., "*La gestione del rischio e la sua comunicazione. Gap teorici ed evidenze empiriche nelle società quotate italiane",* pp. 17-19, Aracne, 2020.

Patten D.M. and Zhao N., *Standalone CSR reporting by U.S. retail companies*, Accounting Forum, Vol. 38, pp. 132–144, 2014.

Prandi P., *Il risk management. Teoria e pratica nel rispetto della normativa,* Franco Angeli, 2010.

Robert G. Eccles, Ioannis Ioannou, and George Serafeim, *The Impact of Corporate Sustainability on Organizational Processes and Performance*, Management Science 60, no. 11, pp. 2835-2857, November 2014.

Rogers, D. A., Managing financial risk and its interaction with enterprise risk management. John Wiley and Sons., 2010.

Segal S*., Corporate Value of Enterprise Risk Management: the next Step in Business Management*, Hoboken, New Jersey: Wiley, 2011.

Singer T. and Tonello M., *The Business Case for Corporate Investments in ESG Practices,* The Conference Board Inc., July 2015.

Singer T. and Tonello M., *The Business Case for Corporate Investments in ESG Practices,* The Conference Board Inc., July 2015.

Singer T., *Driving Revenue Growth Through Sustainable Products and Services*, Research Report No. R-1583-KBI, The Conference Board, June 2015.

Sorin G. and Anca E., *Enterprise risk management: a literature review and agenda for future research*, Journal of Risk and Financial Management, Vol. 13 (281), pp. 9-15, 2020.

SRA, Society for Risk Analysis, definition provided in the glossary, 2018.

Stubbs W., Higgins C., *Stakeholders' Perspectives on the Role of Regulatory Reform in Integrated Reporting*, Journal of Business Ethics, Vol. 147(3), pp. 489-508, 2018.

The paper takes into consideration the analysis conducted by Beasley M.S., Branson B.C., Hancock B.V., *"ERM: Opportunities for Improvement",* Journal of Accountancy, vol.1 September, pp. 28-32, 2009.

Tarallo P., *La gestione integrata dei rischi puri e speculativi,* Franco Angeli, 2000.

United Nations, Report of the World Commission on Environment and Development, *Our Common Future*, New York: Oxford University Press, 1987.

Venturelli A., Caputo F., Cosma S., Leopizzi R., Pizzi S., *Directive 2014/95/EU: Are Italian Companies Already Compliant?,* Sustainability, 9, 1385, 2017.

Williamson D., *The COSO ERM framework: a critique from systems theory of management control*, International Journal of Risk Assessment and Management, Vol. 7(8), pp. 1089-1119, 2007.

World Economic Forum, *The Global Risks Report 2018, 13th Edition*, Retrieved from World Economic Forum: reports.weforum.org/global-risks-2018/, January 17, 2018.

Xueming Luo and C.B. Bhattacharya, *Corporate Social Responsibility, Customer Satisfaction, and Market Value*, Journal of Marketing 70, no. 4, pp. 1-18, 2006.