Haute Ecole

« ICHEC – ECAM – ISFSC »

Enseignement supérieur de type long de niveau universitaire

Risk transformation: study of the challenges and opportunities for the non-financial sector.

Mémoire présenté par :

Antoine BEERNAERTS

Pour l'obtention du diplôme de:

Master's degree in Business Management

Promoteur :

Stéphane NOLF

Boulevard Brand Whitlock 6 - 1150 Bruxelles

I, the undersigned, BEERNAERTS, Antoine, Final year in the MIBM program, hereby declare that the attached thesis is free of plagiarism and complies in all respects with the study regulations on borrowing, citation and use of various sources signed when I registered at ICHEC, as well as the instructions concerning referencing in the text complying with the APA standard, the bibliography complying with the APA standard, etc.". made available to me on Moodle. By my signature, I certify on my honour that I have read the aforementioned documents and that the work presented is original and free of any borrowing from a third party not properly cited".

Date and Signature:

Woluwé Saint-Lambert, May 19th 2022

Acknowledgements

Writing this thesis has taken an amount of time I would not have imagined before, but I certainly cannot take all the credit for this last assignment ending a 5-year journey at ICHEC.

First of all, I would like to thank Olivier Elst and all his team at KPMG for guiding me into the world of risk management and offering me the possibility to be involved in such an interesting project. Their patience and understanding with me have helped me come to this document and I am most grateful for this.

Secondly, my thanks go to my promoter Mr Stéphane Nolf who reviewed my thesis and pointed me towards the right directions when I could make sense of what was not right.

I could not have gone through this period without my girlfriend Emilie, who besides her constant support and kind words, did not hesitate to remind me of my delay by showing me the status of her own thesis.

Lastly, I want to thank my parents for supporting me every day of these 5 years at ICHEC and for not having doubted me for a second even when I switched studies in 2017; I certainly could not have done it without them.

Table of Contents

1. Introduction

Never before have organisations operated in such an uncertain and dynamic risk environment. Indeed, the environment in which they evolve is unprecedented as every key aspect of businesses is currently evolving in its own way in line with the trends of modern economy. This is even more true today as uncertainty has become a standard in our daily lives and in the lives of the organisations that surround us. Therefore, the way risks will be managed plays, more than ever, a key role to ensure viable and sustainable growth. This is evident in the way that the approach to risk management is shifting from being reactive to being more proactive and dynamic. This shift is risk transformation. This movement is described by ISACA (2019) as *"the continual evolution of an organization's risk function, systems and processes".* We know and see that approaches to risk management are multiple and that there is no 'one size fits it all' model; companies have realised that given the current risk landscape, building increasingly efficient risk management models is the next step in risk transformation to operate successfully. While companies remain free to choose the approach to risk management that best fit their business model, one can easily understand that updating and transforming this approach has become a real necessity for companies around the world given this ambiguous risk landscape that has built up. This necessity is even more true for companies operating in the non-financial sector as they are not subject to regulators like financial companies are, creating a wide space of operating possibilities in terms of risk management. This thesis will present the challenges and opportunities that come with risk transformation.

The first section is a theoretical approach covering the relevant aspects of risk management. We will first cover the concepts of governance through the two most widely used risk management frameworks, namely the COSO Enterprise Risk Management framework and the ISO 31000: Risk Management framework. Leading concepts such as the 'three lines model' of the Institute of Internal Auditors and the notion of crisis management will also be reviewed. Secondly, we will review the main risk management processes, before presenting a concise literature review on the expected evolution of risk management practices in the years to come.

The second section of this thesis will challenge the concepts developed in the first section through a practical approach to risk management. This was made possible thanks to a study around risk transformation we conducted during our internship at KPMG Belgium from September 2021 to May 2022, hereafter referred to as "the Study". Results from this Study will be analysed and presented under the format of a report, highlighting the challenges and the opportunities deriving from current risk management practices and their expected evolution within the next five years.

Finally, this thesis will be concluded by a summary of the key findings from the Study that will walk the reader through the key trends and ideas that were identified during the processing of the data.

2. Theoretical approach to risk management

Risk transformation encompasses many concepts which are necessary to study in order to understand all the findings brought forth by the Study conducted around this topic. As such, we will first review the various theoretical aspects needed to understand the risk management environment and what it is made up of, and then the most widely used risk management frameworks to see what guidelines these offer to companies. Indeed, the ISO 31000: Risk Management is used in more than 70 countries, while the Committee of Sponsoring Organization of the Treadway Commission 'COSO' Enterprise Risk Management framework, which was jointly developed by COSO and Price Waterhouse Cooper, is supported by most major consulting firms (Williams, 2020). Main risk management processes and linked concepts will then be reviewed.

This approach will help us understand what the best practices are and how companies follow them today. These insights will provide us with the necessary foundation to see the sort of approaches companies are headed towards within the next five years.

2.1 Glossary

Risk management: The International Standards Organization completes this definition by stating in the ISO 31000 that risk management is made up of "*coordinated activities to direct and control an organization with regard to risk*" (ISO, 2018) .

Enterprise risk management: The COSO Enterprise Risk Management framework (ERM) goes further in the definition of risk management by describing it as "*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 risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives" (Compliance Online, n.d).*

Non-financial sector: The European Commission gives us a definition of the non-financial sector as follows: *" The non-financial corporations sector is an institutional sector in national accounts. Institutional sectors within national accounts bring together economic units with broadly similar characteristics and behavior. It consists of institutional units which are independent legal entities and market producers, and whose principal activity is the production of goods and non-financial services. It may be divided into three subsectors covering: public non-financial corporations; national private non-financial corporations; foreign controlled non-financial corporations"* (OECD, 2022).

Financial sector: "*set of institutions, instruments, and the regulatory framework that permit transactions to be made by incurring and settling debts; that is, by extending credit."* (OECD, 2022)

Risk: a risk is "*an effect of uncertainty on objectives*". In this regard, an effect should be according to ISO considered as "a deviation from the expected, that can be positive, negative or both, and can address, create or result in opportunities and threats" (ISO, 2018)

It is important that several elements are necessary to analyse risk, those being the risk source, potential events, their consequences and their likelihood (this approach is the most basic one and will be complemented by new elements along the thesis, but basic risk analysis cannot be initiated without these elements).

According to ISO, the following terms are defined as follow:

Risk source: "*element which alone or in combination has the potential to give rise to risk*" (ISO, 2018)

Event: "*Occurrence or change of a particular set of circumstances. An event can have one or more occurrences and can have several causes and several consequences. An event can also be something that is expected which does not happen, or something that is not expected which does happen. Lastly it can be a risk source*" (ISO, 2018).

Risk appetite: "*the amount and type of risk that an organization is prepared to pursue, retain or take*" (ISO, 2009)

Consequence: "*Outcome of any event affecting objectives. A consequence can be certain or uncertain and can have positive or negative direct or indirect effects on objectives. Consequences can be expressed qualitatively or quantitatively. Any consequence can escalate through cascading and cumulative effects*." (ISO, 2018).

Likelihood: "*In the risk management terminology, the word "likelihood" is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period)*" (ISO, 2018).

This brief introduction to risk management related terminology serves as foundation for the theoretical approach that we will now present, but those elements will also be used in the analysis of the Study during the practical approach of the thesis. We will now review the key concepts used in the Study led around risk transformation and that will be useful to understand the matters at hand with more depth.

Development of those concepts will start by looking at the concept of governance within risk management and what it stands for, by reviewing the core principles of the COSO Enterprise Risk Management Framework and of the ISO 31000 – Risk management framework. We will then describe risk management processes through the lens of those two frameworks as well, although we will complement this description with additional information and insights gained through our Study.

2.2 Governance

Governance is a fundamental aspect of risk management, considering the way a company is governed will in turn dictate how the different activities that it undertakes are managed. Governance therefore includes the way a company is organized and how exchanges should occur to allow the business to operate smoothly, with all the actions and the decisions being taken on the basis of the relevant information treated by the relevant people.

Companies can rely on local codes of governance to find guidance, but the COSO Enterprise Management Framework and the ISO 31000 – Risk management framework offer a generic view of the governance structures that organisations could adopt in order to have a well-functioning risk management.

Therefore, we decided to explore both frameworks to develop a broad view of the organisational setup recommended by those two leading organisations in the risk management field that are COSO and ISO.

2.2.1 The COSO Enterprise Risk Management framework.

Scope of the COSO ERM framework

The COSO ERM framework, which stands for Committee of Sponsoring Organization of the Treadway Commission is not only a framework of tangible elements and concepts linked to Enterprise Risk Management, but also an approach of how risk should be approached generally. It therefore offers a view on how risk should be treated within all the operations of a business.

The notion of Enterprise Risk Management goes a step further in the definition of risk management, and describes it as "*a process, affected 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 its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives*" (COSO, 2004).

According to Morgan (2021), this approach differs from traditional concepts of risk management, which can be described as very formal, with risk management being considered as a business function separate from the others. ERM however, approaches risk management from a more proactive point of view by making discussions within the company happen, which would not be the case in a traditional silo approach which is more a reactive posture companies can adopt.

It is commonly considered that the management function within a company is to a certain extent responsible for managing the risks the company faces. However, according to the COSO framework, risk management should not end there. Enterprise risk management should be seen by the board and stakeholders as a competitive advantage in its own right. To achieve this, management should enhance its dialogue with these two organs.

According to COSO, moving in this direction would afford management a better view of how risk should be considered in relation to the strategy and the impacts it could have on it. The addition of the risk dimension within the strategy will help take the strengths and weaknesses of the company into account, and in turn demonstrate how well the strategy matches with the mission and the vision a company has for itself. This approach builds up more assurance for the management that the right strategy has been selected from the different options and alternative strategies available.

Regarding the role of the board, COSO considers it as an oversight role whose aim is not only to support value creation for the company, but also to make sure that it does not endure the negative impacts that can derive from a risk event, which can be financial, reputational, or organisational. While risk management has, in the past years, been a support activity for the board, it is increasingly considered that risk management is an element that should be taken into consideration by every member of a company, regardless of their position. This is a clear sign of risk transformation, meaning that the attitude and approach to risk management is changing.

The oversight responsibilities of the board are defined and addressed within the COSO framework through various dimensions: "*governance and culture; strategy and objective-setting; performance; information, communications and reporting; and the review and revision of practices to enhance entity performance*" (COSO, 2017).

We find, in the COSO framework, a comprehensive but not exhaustive list of what these oversight responsibilities can be.

The framework suggests that the strategy proposed, as well as the risk appetite, should go under review and be challenged by the senior management, implying a thorough knowledge of risk management to understand and validate the strategy the organisation should adopt. This aims to align the strategy the company will pursue with its business objectives so that it is in line with the company's vision, values and mission.

Taking significant decisions regarding the future of the company is one of the core activities of the Board, and it is the responsibility of their members to ensure that senior management realigns the practices that deviate from the values and strategy of the organisation. The framework also highlights the fact that the Board is responsible for the good relations with both the investors and employees, by managing the incentives and remuneration in line with the job's requirements.

With regards to strategy and objectives setting, the COSO framework states that "strategy selection is all about making choices and accepting trade-offs" (COSO, 2017). Therefore, risks play a major role in this process as it is a key element for the Board to consider in making informed decision in relation to strategy.

The way this topic is often approached is by assessing how a risk could affect the existing strategy, the focus is usually on the direct effects a risk can have. However, it is suggested by the COSO that risk management models followed by organisations are becoming more customer centred than before as well as more dynamic, indicating that risk is becoming a key driver in strategy statements.

Misalignment of the strategy with the values, vision and mission of a company is a challenge faced by companies. Therefore, the selection of the strategy becomes a key decision.

While some companies do not believe this is an important point to consider, it has been proven that having a strategy which reflects the "mission, vision and core values" (COSO, 2017) of the company plays an important role in building resilience during times of changes.

Indeed, not having a strategy supporting the mission and vision of an organisation could prevent an organisation from reaching its objectives or even realizing its mission and vision at all. For that reason, the COSO framework considers the strategic aspect of the risk management approach as a central element in strategy selection.

Selecting a strategy involves choosing out of multiple alternatives, each with their advantages and disadvantages. Those advantages and disadvantages of each option reflect the risks involved, hence the importance of enterprise risk management given the different outcomes each choice can provide. It is therefore the role of the Board and of the management to determine which strategy has a risk profile that best matches the risk appetite of the company, but also its core values, vision and mission. This implies that senior management requires a thorough understanding of risk management to evaluate and validate the strategy the organisation should adopt. Finding the most appropriate strategy will in turn help the organisation reach its objectives and make an efficient use of its resources (COSO, 2017)

Considering the above, it is stated that risk management is not only about managing risks but also, as developed in this section, about understanding the implications of an inadequate strategy for the viability of a company's activities (COSO, 2017).

According to the framework, enterprise risk management should be seen as an opportunity for companies to support the achievement of their objectives and the realization of their vision and mission.

One will see along this thesis that the governance aspect plays a very important role within risk management, but risk management has an equally important role within governance as the COSO framework suggests it, considering how it affects the way operations are run. As such, defining the central role of ERM within the strategy choice of a company was essential to a good understanding of its necessity and its broader implications (COSO, 2017).

According to COSO, enterprise risk management plays a role in the way a company can face uncertain events and changes in its environment. Indeed, a strong risk management framework helps companies to identify new trends that could either lead to the occurrence of a risk, but also to changes in their environment which could have as consequences the deviation from the objectives or an impact on the organisation's performance. The clarity provided by a well-defined framework provides companies with planning opportunities and more chances to adapt their strategy early and therefore be able to react quickly (COSO, 2017).

Highlighted benefits of the COSO ERM framework.

As established above, a sound risk management framework offers organisations the opportunity to capitalise on their strategy by harnessing the opportunities created by the fast-changing environment they evolve in. A number of benefits of sound risk management in relation to strategy selection are listed by the COSO as follows.

Firstly, an enterprise risk management framework increases the number of opportunities a company can harness. Indeed, acquiring the ability to take all possibilities into account (hence the ability to plan better) allows organisations to build a global view of the negative and positive impacts changes can have on the company.

This clarity provides them with the ability to turn these elements into opportunities by clearly identifying rising challenges. It is believed that being able to manage risks efficiently provides companies with the ability to better identify risks, making room for more appropriate mitigating measures, reducing costs, losses and surprises (COSO, 2017).

Secondly, a clear risk management framework provides companies with a structural stability. Indeed, considering the interconnection between risks and the fact that those same risks can originate in any part of an organisation, making sure that they are managed efficiently protects companies from suffering entity wide impacts and therefore also ensures a performance stability (COSO, 2017).

The anticipation of risks can also help companies to turn apparent threats into opportunities when it is feasible. Indeed, the COSO framework argues that all risks represent a request for resources.

Therefore, being well-informed about the risks faced by company enables its management to evaluate the resources required to face those risks and optimize their resources allocation depending on the company's priorities (COSO, 2017).

Then, the concept of resilience is also observed to be enhanced by the presence of a strong risk management framework. The ability of a company to be viable on the long term lies in its capacity to face change. Enterprise risk management is therefore a strong tool that helps organisations not only to survive, but also to thrive within their changing environment. Given the accelerating pace at which businesses change, this dimension of resilience is to be taken into consideration (COSO, 2017)

All these elements demonstrate that risks should be viewed as catalysts of change, as they create opportunities for businesses by creating chances to differentiate and evolve with the environment of the company. As such, they should not only be seen as challenges by the organisations, but as a way to move forward (COSO, 2017).

Dimensions of the COSO framework

As stated, the COSO framework brings clarity to companies regarding the importance of risk management within strategic planning activities. The omnipresence of risks within a company's environment makes it an important aspect to consider and the COSO framework itself helps companies to face their risks thanks to a set of five components: **"Governance and Culture; Strategy and Objective – Settings; Performance; Review and Revision, Information, Communication and Reporting"** (COSO, 2017).

Governance and culture:

This part of the COSO framework sets the best governance practices by recommending what the oversight responsibilities should be with regards to risk management. The Board should support the achievements of the organisations' objectives.

Regarding the cultural aspect of this component, it relates to the way risk should be understood within organisations, as well as to the behaviours that should be adopted to be in line with this understanding. It is therefore important that a strong commitment to the values of the company is demonstrated.

In order to reach those goals, the Board should also choose an appropriate structure for their risk management which will carry out the necessary tasks. The company should find the right profiles to complete their teams and retain the most capable ones (COSO, 2017).

Strategy and Objectives – Settings

The framework recommends companies to make sure their risk appetite is aligned with their strategy, and in turn to implement concrete actions to start managing the risks linked to this strategy. The definition of a risk appetite should be made based on the context of the company; the potential impacts related risks could imply; but it also on the willingness of the company to maintain its value creation goals.

Those actions will be, with regard to risk management, aimed at identifying, assessing and responding to risks. Organisations should also continuously consider what the other alternatives are to their current strategy and what impacts implementing those strategies could have on their operations.

Lastly, companies should make a clear formulation of their business objectives based on their strategy (COSO, 2017).

Performance:

As stated in the previous framework component, risks that could lead to a deviation from the strategy have to be identified and their potential impacts should be assessed. Note that risks should be prioritized depending on the amplitude of the impact it could cause to the company.

Depending on where they are located compared to the risk appetite, adequate actions and controls should be taken and a portfolio of the risks taken by the organisation should be created to keep the stakeholders informed of the current situation the business is facing (COSO, 2017).

Review and revision

The review of an organisation's performance allows companies to see which parts of its risk management framework are efficient, and which ones are not. Based on this, necessary revisions can be made to reach the objectives and remain within the risk appetite boundaries.

Moreover, those revisions can also occur because of important changes identified and assessed by the company as part of the monitoring of their strategy and objectives (COSO, 2017).

Information, communication and reporting

According to the COSO framework, continuously gathering information both from internal and external sources is an essential component of enterprise risk management. The flow of information is a critical element of the governance of a company. Technology plays a determining role in this aspect, as it provides overseeing organs with more opportunities than ever to rely on accurate and extensive information. Information should be communicated through all the layers of the company through the relevant channels to support risk management activities across the company (COSO, 2017).

One should however bear in mind that the COSO framework offers a view on how governance can impact risk management activities, but all processes implemented have to be defined by the companies depending on their needs and objectives.

While COSO offers an approach used by a large number of companies, other framework like the ISO 31000 on risk management are also considered as industry standards and should therefore also be studied (COSO, 2017).

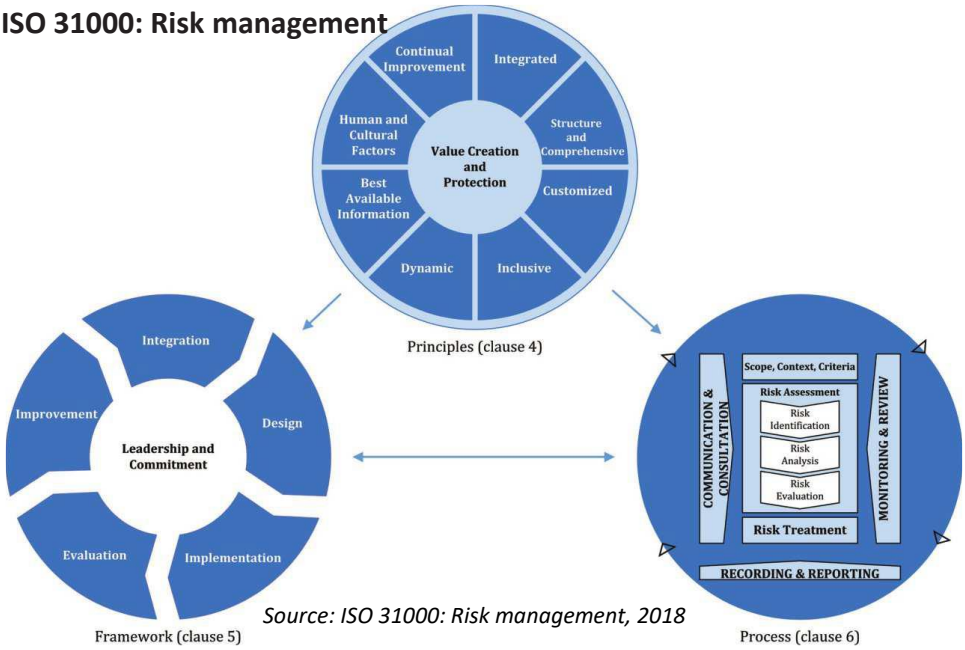
2.2.2 ISO 31000: Risk management

Like the COSO framework, the ISO 31000: Risk management is meant to guide companies to choose the right strategy and reach their objectives based on well-informed decisions. As such it is used by organisations to sustain and improve their results by considering the external and internal elements that could impact the company's activities.

As mentioned in the preamble of the framework, managing risk is a part of the governance activities of a company. It plays an essential role in managing the company as a whole. It requires companies to study their internal and external environment as well as human factors and the culture of the company.

According to the ISO framework, a number of principles enable companies to manage risks as shown in the picture hereunder. One can see that risk management is a concept which interconnects many elements. It can therefore be considered a fundamental part of the foundations of a company, and it should be operated efficiently to ensure the viability of a company (ISO, 2018).

Figure 1: ISO 31000: Risk management



Source: ISO 31000: Risk management, 2018

Elements proposed by the framework should however be adapted to each company's particular contexts. The interconnection between those elements with risk management however remains the same.

The principles and the framework itself will be reviewed in this section, while the processes will be dealt with systematically later in the thesis. This will ensure a total coverage of the elements necessary to tackle the topic of the thesis in line with the structure set out in the introduction.

In order to make a comparison between the COSO ERM framework and the ISO 31000 Risk Management framework, we will now describe the core principles of the ISO framework in order to highlight the potential differences in the approach and point out the similarities and differences.

Principles

According to ISO 31000, risk management's objective is to simultaneously sustain and increase the value of a company. Indeed, risk management supports the evolution of companies towards higher performances and innovation, and therefore towards the realization of their goals.

8 principles are provided by the ISO 31000 framework as shown on figure 1 as follows:

- Integration

Risk management should not be considered separately from the other activities of the companies. Indeed, it is a central element to all decision-taking processes which should therefore be considered in each part of an organisation. As a result, risk management should be a part of every process of a company, and every member of management should hold responsibility for the risks they encounter (Learn31000, 2022).

- Structure and comprehension

Having a clear and structured approach to risk management ensures that the company has results in line with the framework in place, but it also supports a shared comprehension of all the employees involved in risk management activities. Moreover, guidelines and procedures give companies the assurance that a certain level of efficiency is maintained (Learn31000, 2022).

- Customization

Each company has a situation of its own. This is why risk management practices should be adapted based on the environment the organisation operates in. To do so, internal and external elements should be taken into account to determine which processes would fit the company best. Considering those elements helps companies decide what their objectives are, to better tailor their risk management to achieve them (Learn31000, 2022).

- Inclusiveness

According to ISO 31000, gathering the different views, approaches and knowledge detained by the company's stakeholders represents an assurance for the company to have a relevant risk management system which mirrors the organisation's current environment. Inclusion also means that stakeholders should not be kept away from risk management activities as they are meant to be transparent. Making sure they are part of those activities means that appropriate language should be used to make sure that all information is passed on and understood (Learn31000, 2022).

- Dynamism

Environments companies evolve in constantly change and therefore require constant monitoring. It is the goal of risk management activities to give appropriate responses to changes a company may face, at an appropriate time, to make sure that the organisation's performance is not affected by them. Risk management should not be a reactive discipline but rather a proactive one. Risks will appear, evolve and disappear with the events a company faces, anticipation is therefore essential to an efficient risk management system (Learn31000, 2022).

- Best availability of information

Having all the information a company could need is virtually impossible, but still organisations should ensure that they have the best available data at their disposal. This means that both historical and current data should be gathered, and like in any methodology, the company should be aware of the limits the information collection process represents and take it into consideration. Still in an effort of transparency, all those information should be made available to the company's stakeholders, following the principle of inclusiveness (Learn31000, 2022).

- Human and cultural factors

The human behaviour, and the culture employees evolve in is an important factor in risk management. The capabilities of each individuals involved, as well as their aspirations within the company should be considered with regards to how they could interfere with the objectives of the organisation (Learn31000, 2022).

- Continual improvement

Risk management should exist within a continuous cycle of "PDCA: plan, do, check, adjust". It is suggested that the experience built up by a company supports its resilience. It is therefore explained that the factors of change a company meets during its lifetime should be used to improve the risk management processes in place, which will in turn allow the company to continually grow (Learn31000, 2022).

It is stated by the ISO 31000 framework that these principles should be understood as the foundation of an efficient and effective risk management approach. By transposing those principles into actions, businesses should be able to face uncertainties with more confidence and achieve their objectives by having appropriate processes in place (ISO, 2018).

Dimensions of the ISO 31000: Risk management framework.

We will now describe how the present framework should be used by companies to integrate risk management within the other activities. How effective the risk management of a company will be, depends on how well governance is embedded within the decision-making process of the company. Therefore, senior management and all stakeholders should be involved.

As illustrated by figure 1, we will see how the implementation of the framework can support risk management through the different steps of the process, namely "integrating, designing, implementing, evaluating and improving risk management across the organization" (ISO, 2018).

Beforehand, the current risk management activities of the companies should be evaluated to see if some grey areas can be addressed to see which parts of the current framework could be enhanced (ISO, 2018)

Roles of governing organs

The ISO 31000 framework describes the responsibilities of the senior management and the oversight organs. It is suggested that they are responsible for ensuring the integration of risk management within all the activities. They should therefore demonstrate leadership and commitment through various behaviours (ISO, 2018).

Governing bodies are in charge of ensuring that the different elements of the framework are transposed into actual actions activities. They should also be the ones to produce a plan stating how risk management should be approached in the organisation (ISO, 2018).

It should also be made sure that the resources required to follow this plan of action are made available to the teams operating in risk management. Moreover, the individuals involved in risk management should be aware of their accountability based on their level of activity. The appropriate authorities should also be clearly designated for every activity of the company (ISO, 2018).

By taking on this role, governing bodies ensure the alignment of risk management with the "objectives, strategy and culture" (ISO, 2018) of the organisation. It is also suggested that senior management and oversight bodies should understand and assume all the obligations linked to their status, as well as their voluntary commitments that derive from the acceptance of their position.

As governing organs, they should also be the ones tasked with defining a risk appetite that should be respected by every individual within the company, as well as to ensure that the amount of risk that can to be taken is properly communicated and respected by every stakeholder of the company (ISO, 2018).

Furthermore, senior management and oversight bodies should support continuous risk monitoring. Monitoring risks in a systematic way will allow them to adapt risk management so that it matches the current environment of the company and remains effective to face new potential risks (ISO, 2018).

The accountabilities of the senior management and of the oversight bodies however differ in the sense that it is the senior management that is accountable for managing risks directly, while it is the oversight bodies' accountability to oversee risk management activities.

Overseeing risk management activities involves a number of tasks. It is expected of the oversight bodies that they ensure the proper consideration of risks within the company's objectives, which requires them to have a thorough understanding of the risks faced by the organisation depending on the objectives that have been set.

Furthermore, they should ensure that the relevant processes to mitigate those risks are implemented and executed in an appropriate manner. It is also explained in the ISO 31000 framework that the information related to those risks should be communicated throughout the company (ISO, 2018)

Integration of risk management

Each organisation has its own mission, objectives and level of complexity and the way risk management is integrated depends on these elements. Every employee of a company faces risks on a daily basis and should therefore manage them at their own level. The way risks should be managed at each level of competence is dictated by the governance in place and it should be meant to achieve the company's objectives as well as to sustain the performance of the business (ISO, 2018)

The integration of risk management within the operations of a company is a process that should be tailored to the business' needs and approach to its activity. According to ISO, this should be achieved through a dynamic process, complemented by an iterative approach. It is suggested that risk management should be part of every aspect of the company's operations, from the operational ones to the strategic and decision-making ones. (ISO, 2018)

Designing risk management

As explained above, risk management should be customized for the company's context, both internal and external. This exercise requires taking several elements into account.

Those elements are exhaustively listed in the ISO 31000 framework as follows:

Regarding the external context of companies, the first elements that should be considered are the factors to which the company is subject, and which can depend on the organisation's geography. Those factors can be of, as stated in the framework, "social, cultural, political, legal, regulatory, financial, technological, economic and environmental factors" (ISO 31000: Risk management). The different elements influencing the evolution of the company's environment should also be taken into account when they become potential causes of deviation from the business' objectives (ISO, 2018).

Moreover, all the relations the company has, should be taken into account. Those relations can be contractual, or relationships with the stakeholders of the organisation, where the stakeholder's views and expectations from this relationship should be considered.

In addition to that, the interconnections of those relations within the network of the company should also be considered to produce an accurate image of the external context of the company (ISO, 2018).

The approach to understand a company's internal context differs as it is more defined that the external one. This analysis relies firstly on the company's values, vision and mission which are at the heart of an organisation's activities. As such, the governance system, with its set of responsibilities and its defined structure for the company should be clear and well understood to make sense of the internal context a company evolves in. Moreover, it is suggested by the ISO 31000 that the organisation's overall goals, strategy and policies should also be considered, as well as the company's culture which should define its members' behaviours.

Furthermore, the framework mentions that the internal context is also defined by the guidelines, models and standards a company adopts. This element is complemented by the resources of any type of an organisation has access to, as well as the information the company is able to acquire and how it uses it (ISO, 2018).

Lastly, like for the external context, each relation existing within the company, their interconnections and the commitments that derive from them should also be considered (ISO, 2018)

Articulation of the commitment to risk management

It is considered by the ISO 31000 that it is the role of the oversight bodies and of senior management to ensure that members of the organisation are committed to risk management. This should be done through a clear statement of the company's objectives and own commitment to risk management.

Commitment can be defined as what a company intends to achieve through its risk management and how it is connected to the organisation's objectives and guidelines. Commitment to risk management also involves the efforts of governing bodies to shape risk management into the culture of the company and to make it part of all activities of the company and of the decision-making processes (ISO, 2018).

Within their role, senior management and oversight bodies should ensure the availability of the necessary resources required to achieve an efficient risk management, clarify the responsibilities and accountability of each individual involved and lastly, the company's performance should be measured through the mean of KPI's and later reported to the competent authorities. This is intended to create an improvement area where gaps can be filled, and inefficiencies improved.

Elements linked to commitment should be communicated through all the layers of the company and to the necessary stakeholders to ensure an alignment on this subject (ISO, 2018)

Roles and responsibilities within risk management

It should be made sure by governing bodies that, when necessary, responsibilities, accountability and authority are defined and assigned to the relevant people within the adequate layers of the company. By doing so, risk management is transformed into a shared responsibility across the all the activities of the company. Risk owners should therefore be identified to know who should bear which responsibility and how the authority lines should be arranged (ISO, 2018).

Resources and risk management

The availability of the necessary resources to operate an efficient risk management within companies has been mentioned several times in this description of the ISO 31000 framework. It is indeed a core responsibility of senior management and oversight bodies to ensure the availability of those resources when required for risk management. These resources are declined in several forms. They can be human resources, made up of people and their skills and experiences. Resources are also made up of all the necessary methods, processes, and tools the company has at its disposal, as well as all the knowledge and information the organisation has retained overtime. Resources should also be maintained through adequate trainings. The resources should also be evaluated to see if they still fit the company's constraints (ISO, 2018)

Communication in risk management

A communication approach should be approved and should be intended as a support for the framework. Communicating the relevant information to the right parties is an important element of an adequate risk management implementation. This implies communicating with the right people at the right time; and the other way around, feedbacks should be provided by stakeholders to enhance the activities. The methods used to communicate should be relevant and fit the company's needs. Information should be passed on and shared in an appropriate format that is understandable and meaningful to all the people it concerns, to ensure sound decision-making processes and provide an improvement area (ISO, 2018).

Risk management implementation

An efficient implementation of a company's risk management should be planned according to the time required by the various processes and the available resources. It should also be decided by who, when, where and how the different decisions should be taken within the organisation. It is also important to note that the ISO 31000 suggests that when necessary, decision-making processes should be reviewed and adapted when necessary. Lastly, a clear understanding of the risk management practices implemented across the company.

Stakeholders are a central element of the success of the implementation of risk management. In turn, a successful implementation gives companies more assurance regarding their capacity to address uncertainties in the future and ensure companies' performance by making sure risk management is part of all the activities across the company and that potential evolution of the company's environment is taken into consideration when necessary (ISO, 2018).

Risk management evaluation

Risk management should be evaluated in terms of effectiveness to make sure it is adequate for the organisation's activities. To do so, the performance of the framework in place should be measured on a periodic basis and based on the objectives and limits set earlier. KPI's should be used, as well as other measurements to evaluate how close behaviours encountered within the company are compared to the ones expected. Those elements should give the business the necessary elements on whether the framework in place is sufficient to support the achievements of the company's objectives (ISO, 2018)

Improvement of risk management

Risk management should continuously be improved based in monitoring of its performance and of the changes in the internal and external contexts of the company. To do so, the company should continually review if the integration of risk management is adequate and if it is still suited for the organisation's reality. Once improvements areas have been highlighted, it is suggested that the company develops plans and actions, which once assigned to the adequate person and implemented, should help enhance the risk management function within the company (ISO, 2018).

2.2.3 Similarities and differences between the COSO ERM framework and the ISO 31000: Risk Management framework.

Having seen the main aspects of both frameworks, it is interesting to see in what way they converge and differ to understand how they can bring a complementary added value to companies implementing them.

According to Carol Williams (2020), three main similarities can be highlighted when comparing the two frameworks. Firstly, one can see that both concepts take the idea of risk to a next level by pushing organisations to embrace risk taking and not considering them only as threats that should be avoided, although ISO 31000: Risk Management is often considered to go more in this direction than the COSO Enterprise Management framework.

Secondly, one should consider the two frameworks as guidelines that should be modelled around companies' needs. Indeed, as mentioned in the introduction, there is no 'one size fits it all' model when it comes to risk management. Therefore, it remains the duty of a company to shape this standard to its environment, keeping in mind that they are not to be applied to the letter (Williams, 2020).

Lastly, and this is probably the most important similarity between the two frameworks, is the fact that they both support the integration of risk management within the decision-making processes at each level of the companies, even though Williams notes that the ISO 31000: Risk Management is more insistent on the topic (Williams, 2020).

Considering the differences now, Williams notes that the two frameworks have from the beginning a different approach to the subject of risk management. Indeed, the COSO Enterprise Risk Management framework brings more insights about the role of the Board within the risk management field, but it does not discuss the risk management processes in depth. ISO 31000: Risk Management on the other hand, has a clear focus on risk and its inclusion within the strategic planning of the companies using it. In this sense, ISO strictly makes a difference between the framework within which a company evolves, and the processes which are clearly defined (and will be discussed later in this theoretical approach). COSO offers a combination of these two areas of interest but remains vaguer (Williams, 2020).

2.2.4 The three lines models.

The three lines model, which was originally called the three lines of defence model when it first originated in 2013 from the Institute of Internal Auditors[1] (IIA), is regarded as one of the most efficient tools in terms of risk management by people active in governing bodies and internal audit. The evolution of management and of the environment in which companies evolve, has pushed the three lines of defence model to evolve itself and leave behind the idea of defence to display an approach which is rather proactive than reactive. As such, it also supports a strong collaboration among all actors involved in a company's risk management (Institute of internal auditors, 2022).

Considering the influence it has gained since its birth in 2013, we believe that presenting the principles of the three lines model is essential as it will also be reviewed in the Study later in this thesis.

As explained in the preamble of the updated three lines model of the IIA, companies are currently evolving in an increasingly complex, unpredictable and globalized environment. Organisations also have to take into account the needs of their various stakeholders, which are most often not aligned and can change overtime.

As described in previous sections, governing bodies receive guidelines from the company's stakeholders regarding the oversight activities that should be undertaken. It is however management that is entrusted with the resources and the authority to tun the day-to-day operations and decide which actions should be taken, as it is the case for risk management activities.

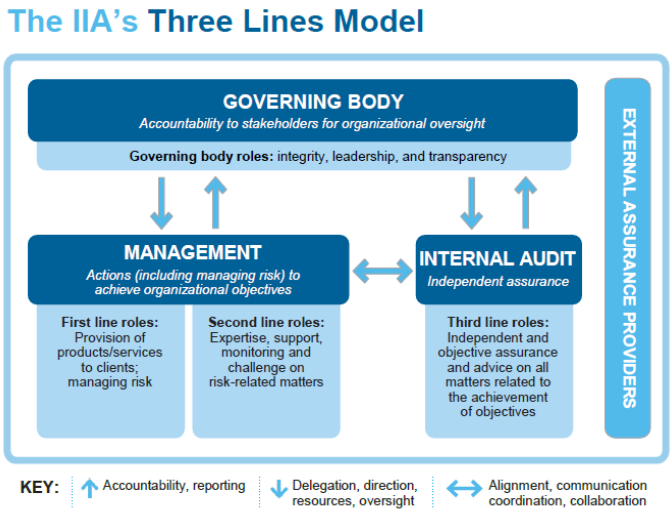
In response to the challenges posed by the environment companies evolve in, it is suggested by the IIA that governance and risk management should be supported by adequate structures and processes ensuring the accomplishments of the companies' goals. As such, governing bodies are the ones to whom management report, like internal audit does independently to provide objective assurance (Institute of Internal Auditors, 2022).

In this context, the Institute of Internal Auditors puts forth the three lines model which gives companies guidelines on how to design their structures and processes. The model is not limited to a particular type of organisation and can support the foundation of a strong governance as well as of risk management. When it comes to implementation, the IIA states that their principle-based approach, which will be developed hereunder, can help companies pursue their objectives. Moreover, it is believed that adopting the three lines model can support value creation and protection within risk management in companies that implement it.

[1] "Organization which advocates, provides educational conferences, and develops standards, guidance, and certifications for the internal audit profession" (Institute of Internal Auditors, 2022)

It is however required that companies clearly set the responsibilities and accountabilities of the different parties of this model, as well as their relationships (Institute of Internal Auditors, 2020).

Figure 2: The IIA's Three Lines Model



Sources: Institute of Internal Auditors, 2020

Principles of the three lines model

According to the IIA, the success of the three lines model relies partly on the principle-based approach it offers. These principles are, respectively, "governance, governing body roles, management and first and second line roles, third line roles, third line independence and lastly, creating and protecting value" (Institute of Internal Auditors,2020).

Governance

The first principle developed by the IIA targets the structures implemented within companies, as well as the processes in place. Those elements give insights on the accountability governing bodies hold towards their stakeholders. They should therefore show integrity and display a transparent behaviour.

The governance of the organisation should also be demonstrative of the actions taken by management to pursue the company's goal and allocate the necessary resources to do so. Lastly, the governance structure should ensure that an independent internal audit function is present to make sure that an objective perspective on the risk management practices is communicated and in turn provide the business with improvements opportunities (Institute of Internal Auditors, 2020).

Governing body roles

According to the IIA, governing bodies are tasked with implementing the adequate processes and making sure the right structures are in place to ensure an efficient governance. They are also the ones in charge of having made sure that the interests of the stakeholders are well represented within the organisation's objectives.

Regarding the day-to-day operations, the three lines model suggests that the governing bodies should let management allocate the necessary resources and take on the responsibility to achieve the organisation's objectives. Management should make sure all expectations are met regarding legal, ethical and regulatory aspects (Institute of Internal Auditors, 2020).

The third, fourth and fifth principles will be developed according to the different lines of defence for a matter of clarity.

To start with, we will describe the roles of the different lines present in the model. We will then focus on the relationships between the different lines.

First line function:

The first line represents the operational line management (Lyons, 2020) that deliver products or services, depending on the company. Support activities are also considered to be part of the first line. These activities are the ones practically managing risks on a daily basis. As such, they are held responsible for effectively managing risks.

From a practical perspective, first line officers are the one to take the actions and responsible to use the necessary resources that are at their disposal to ensure that the objectives of the company are reached.

Taking on these responsibilities require them to have a constant dialogue with governing organs. This means that based on the course of action they choose to follow, first line officers should report on the outcomes and see whether or not they fit with the company's objectives (Institute of Internal Auditors, 2020).

Second line function

The role of the second line represents the tactical oversight function (Lyons, 2020); and is there to facilitate risk management activities by providing assistance to the first line of defence.

The main task of the second line of defence is to "focus on specific objectives of risk management, such as: compliance with laws, regulations, and acceptable ethical behaviour; internal control; information and technology security; sustainability; and quality assurance" (Institute of Internal Auditors, 2020).

The expertise brought by the second line officers helps "support, monitoring and challenge" risk-related activities. Namely, they are the ones that define the activities that should be carried on by the first line of defence regarding risk management and internal control. It is at this level that the decision is made on which processes are adequate for the needs of the company (Institute of Internal Auditors, 2020).

They also have a reviewing role as they should control the good functioning of the processes in place in risk management and internal control (Institute of Internal Auditors, 2020).

Third line function

The third line, internal audit, is the function tasked with providing objective and independent views on the efficiency of the governance within the company, as well as the one of the risk management activities and internal control. These observations are the results of precise processes led by experimented people; and the results these processes provide support the organisation in the improvement of its operations. The assurance provided by the third line of defence is essential to the model described as it provides governing bodies with an unbiased view on the processes occurring in their business, but also assurance on the providers the company deals with, either internal or external ones. This independence allows internal audit not to be influenced by responsibilities like it is the case for management functions. In order to complete its task, internal audit should have the adequate access to resources they require, but also to people, data or any material that could be necessary for them to complete their work and deliver conclusions that are complete and unaltered in terms of judgement (Institute of Internal Auditors, 2020).

Relationships within the three lines model

The original three lines of defence model proposed by the IIA has recently been reviewed to stress the importance of collaboration between the three lines (Brasseur, 2020). Indeed, the previous version was judged to be too focused on defensive moves from the internal audit function (Cohn, 2020) and therefore, a more dynamic approach of the model was needed.

The first relations that we will explore are the ones of the governing bodies of the organisations, as described by the IIA. People making up these bodies are the ones that decide of the vision, the mission, and the values that a company carries; and in the case of risk management, they are also the ones setting the risk appetite. Governing bodies should be communicating with management from the first line of defence, on practical aspect such as the outcomes of the processes in place, but also from the second line of defence regarding risk management oversight and planning (Institute of Internal Auditors, 2020).

The line between management and the governing bodies can be thin, and the separation of both varies from a company to another. Indeed, the process of developing a risk strategy can either be assumed by the governing bodies, the second line of defence, but a joint effort can also be observed in some cases. This usually depends on the involvement of the CEO of the company in the governance of the organisation. Nevertheless, a certain level of communication between the two layers should always be reached to ensure the effectiveness of the operations (Institute of Internal Auditors, 2020).

Regulators can have requirements for companies such as having a CRO or a CCO in place and reporting to the governing bodies, but this is however not the case the scope of our Study since we will focus on the non-financial sector which is not yet concerned by those regulations.

Governing bodies heavily rely on the judgement of internal audit, which act as a trusted liaison with the activities of the company. Keeping this link intact requires governing bodies to maintain the independence of the third line, hence ensuring the validity of the observations it brings to the discussion. As explained above, the independence of internal audit from the management function is an essential element of the three lines of defence model. This however does not imply that internal audit should not have exchanges with the first- and second-line function. There should be, according to the IIA, frequent communications between those parties to make sure that the observations internal audit is making is adequate for the strategy that is being implemented in the company. Internal audit's activities create a deep understanding of how the organisation operates, which builds up more assurance regarding the recommendations that they may have for governing bodies (Institute of Internal Auditors, 2020).

The relationship between the first and second line is one that is often misunderstood. Indeed, the second line of defence is often seen as an oversight function rather than a support function (Vaishnav, 2022), but building up trust through review and improvement processes is very important for the improvement if risk management within companies.

The collaboration between those lines is very important for the operations and the strategy to go well, as a lack of communication can lead to duplication of efforts, creation of gaps in the processes and eventually a loss of efficiency and of assurance which can be damaging for the company (Institute of Internal Auditors, 2020).

While each line has its own distinct tasks and responsibilities, the strengths of all organisations remain the communication the different parties have. Indeed, this ensures sound operations and a high level of efficiency as duplication of efforts are avoided and every action taken is aligned with the decided strategy (Institute of Internal Auditors, 2020).

2.6.2 Critical view of the three lines model

Prof. Dr. Marc Eulerich reviews this updated three lines model through a critical discussion based on the differences and similarities with the first version of the three lines of defence model published in 2013 by the Institute of Internal Auditors.

According to Eulerich, the three lines model put forth by the IIA offers a great scope for companies to operate in as it enables organisations to have a high level of flexibility regarding the way they build their governance structure.

This liberty, according to the author, gives each company applying the three lines model the chance to customize it as best suits the company's specificities; but it can also be seen as reducing the overall efficiency of implementing a precise framework. Indeed, the framework's guidelines remain vague and leave room for interpretation on the companies' side. It is therefore suggested by Eulerich to consider the three lines model as a supporting concept for an efficient risk management rather than a set of rules to follow strictly. One should understand that the company's specific environment will influence the way the model is implemented and that its words should not be interpreted in absolute (Eulerich, 2020).

According to Jonathan Howitt, time should also be taken into account when considering the three lines model. Indeed, the framework can look like an easy thing to implement from a first perspective, but it has been observed that companies having a structure like the one described in the document from the IIA built their structure overtime (Howitt, 2021).

A potential setback of the three lines model, according to Howitt, is the fact that the second and third lines can potentially work in an uncoordinated way, controlling the same processes and starting a spiral of 'checkers of checkers', as the author refers to it.

The duplication of effort represents a waste of resources which is not aligned with the objectives of the three lines model, but coordination of the three lines is a complex organisation to implement. Changing the habits of people who previously endorsed control functions can be challenging for a company, and decentralizing risk management activities can sometimes seem like a loss of efficiency even though this is not an absolute reality. Therefore, companies and their employees need to have a clear understanding of the segregation of responsibilities that should be in place in order for the framework to become efficient and avoid duplication of efforts.

The responsibilities as developed by the three lines model should not only be defined by activities, but also by reporting lines in order bring clarity to risk duties ad avoid employees to assume several roles at the same time (Howitt, 2021).

The emphasis on the supporting role of the three lines model should, as a conclusion, be well understood by the companies implementing it. Furthermore, the guiding principles should be thoroughly applied, although leaving room to adaptation depending on the companies' situation, to make sure every role and responsibility is properly understood and applied across the organisation.

2.2.5 Business continuity and crisis management

To address the expected organisational approaches to risk management from a complete perspective, one should also describe the angle of a company's resilience through business continuity and crisis management. Indeed, this has more than ever been a topic of interest given the times we are living. Business continuity and crisis management have become central concerns and have proven to be integral elements of the governance of any organisations. As such, we decided to describe these concepts which will later be reviewed in the Study to see to what extent they are used and how they are expected to evolve.

According to Daniël Pairon from KPMG Belgium, business continuity management can be defined as "a holistic process that identifies potential threats to an organisation and identifies the impacts to business operations that those threats, if realized, might cause" (Pairon, 2020). The purpose of this field is to support companies to build up the necessary capacity to face but also to recover from unpredicted events that can occur.

Recent events like the beginning of the Covid pandemic in 2020, and more recently the war outbreak between Russia and Ukraine has proven that the environment we live in is constantly evolving and that companies should be ready to face any events. Lacking the infrastructures to face those events may eventually lead to business failures. This is why it is advised to have a structured plan which directs the company in case an unpredicted event was to happen (Pairon, 2020).

A business management framework consists, according to Khor et al. (Deloitte), of several steps. First, the current level of readiness for unpredicted events should be analysed, as well as the potential risks that could affect the continuity of the companies' operations and their related impacts.

Based on this, Deloitte suggests that a recovery strategy should be developed and adopted, should a disruption occur. This strategy should be based on the maintain of the company's objectives, as well as on the protection of its people, reputation, value and profit while taking into account the laws and regulations that could restrain their actions.

The strategy should be cost-effective and take into consideration how the various resources from the company could be affected.

For a recovery strategy to be a success, it is essential that the business continuity plan's processes are properly documented and communicated through a clear message that is understood uniformly throughout the organisation (Kohr et al. 2020)

Regarding the implementation of the business continuity management plan, the company should acquire the resources it needs to make its plan feasible. It should also be made sure that security measures, technical solutions and contracts are prepared accordingly to what has been planned. As explained in Deloitte's paper, and corroborated in KPMG's article about business continuity management, great efforts should be put in the implementation phase (Kohr et al. 2020). Indeed, Pairon explains in his article that testing and exercising the business continuity and crisis management plan is an important element of the process as it will ensure the effectiveness of the latter, should it ever be needed (Pairon, 2020).

The last step of the process consists of maintaining and improving the business continuity of a company by reviewing and updating it based on the company's changing environment (Kohr et al., 2020). This part of the process ensures that the stakeholders have a view on how things evolve so that a certain level of transparency is reached (Pairon, 2020).

Pairon states that three distinct documents should be part of the business continuity management of a company:

- The business management plan, which gives directions regarding the actions to take by the management in order to "manage a crisis and recover critical operations" (Pairon, 2020).
- The business continuity plan, which consists of a list of procedures to follow in case a major disruption happened. These procedures include the strategies to implement, who to contact, the resources needed, et caetera.
- The disaster recovery plan, which aims at restoring the most critical activities of the company.

Pairon puts forth elements of success for a business continuity management such as a strong leadership (meaning that a strong support from the top of the organisation is essential for any recovery plans to succeed), the clarity of the documents and procedures making up business continuity management, the awareness of the current capabilities of the company and lastly the fact that relevant documents should be accessible to anyone easily to allow the global involvement of the business.

The implementation step of business continuity management stresses the importance of testing the processes, but another key factor of success is also the readiness of the company to accept change within its practices. While the impact to the company a disruption could have, should be thoroughly analysed, so should the impact it could have on the employees and the measures that should be taken consequently (Pairon, 2020).

2.3 Risk management processes

2.3.1 Risk assessment

According to the ISO 31000, risk assessment is "the overall process of risk identification, risk analysis and risk evaluation" (ISO, 2018).

According to the ISO framework, the knowledge and perspectives of the company's stakeholders should be considered in order to assess the risks the organisation may face in a systematic way and based on the best available information and investigation when necessary.

Risk identification, which is a key part of this part of risk management has as a goal "to find, recognize and describe risks that might help or prevent an organisation achieving its objectives" (ISO, 2018).

In order to identify risks as best as can be done, companies should consider the following elements, as well as their potential interconnection: "tangible and intangible sources of risk; causes and events; threats and opportunities; vulnerabilities and capabilities; changes in the external and internal context; indicators of emerging risks; the nature and value of assets and resources; consequences and their impact on objectives; limitations of knowledge and reliability of information; time-related factors; biases, assumptions and beliefs of those involved" (ISO, 2018).

Once the risks identified, companies should evaluate whether or not elements that could cause these risks to occur are under control and define what the results of those risks could be for their business.

Risk typology:

Risk identified can be of many natures, we will therefore offer an exhaustive risk typology.

Operational risk: “the risk of losses stemming from inadequate or failed internal processes, people and systems or from external events” (European Banking Authority, n.d)

Strategic risk: “a possible source of loss that might arise from the pursuit of an unsuccessful business plan” (Business Dictionnary, n.d)

Compliance risk: “the risk of legal or regulatory sanctions, material financial loss, or loss to reputation a bank may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organization standards, and codes of conduct applicable to its banking activities” (ISACA, 2019)

Fraud and security risk: “fraud risk is the risk of unexpected financial, material or reputational loss as the result of fraudulent action of persons internal or external to the organization” (Open Risk Manual, 2020).

Market risk: “risk of losses arising from movements in market prices” (Bank for International Settlements, n.d)

Liquidity risk: “the risk of incurring losses resulting from the inability to meet payment obligations in a timely manner when they become due or from being unable to do so at a sustainable cost” (Council of Development European Bank., n.d)

ESG risk: “environmental, social and governance characteristics that could negatively impact the financial performance or solvency of an entity, sovereign or individual” (Grant Thorthon UK, 2021)

Cultural risk: “misalignment between an organization’s values and leader actions, employee behaviors, or organizational systems” (Deloitte, n.d)

Third party risk: “potential threat presented to organizations’ employee and customer data, financial information and operations from the organization’s supply-chain and other outside parties that provide products and/or services and have access to privileged systems” (Awake Security, 2021)

Societal risk: "risk to a group of people from the realisation of a defined risk that is the consequence to provoke a socio and political response, which is most often expressed in terms of the frequency distribution of multiple casualty events" (Project Definition, 2015)

Outlook at the risks expected to be identified in the future according to the World Economic Forum

The World Economic Forum global risk report 2021 gives us insights regarding the threats most considered by companies worldwide thanks to a survey covering the critical threats the world would face in the future.

The survey highlights the high representation of societal risks within the answers collected on the short-term basis, while medium-term prospects are more focused on economic risks and lastly long-term expectations highlight future third-party risks (World Economic Forum, 2021).

2.3.2 Risk analysis

The risks identified by companies should be analysed to understand what defines them and assess their level of risk. This process should take into consideration elements such as the source of the risk, its likelihood, the consequences it can have on the achievement of the company's objectives, the scenarios in which it could occur as well as the controls that are or can be implemented to mitigate those risks (ISO, 2018).

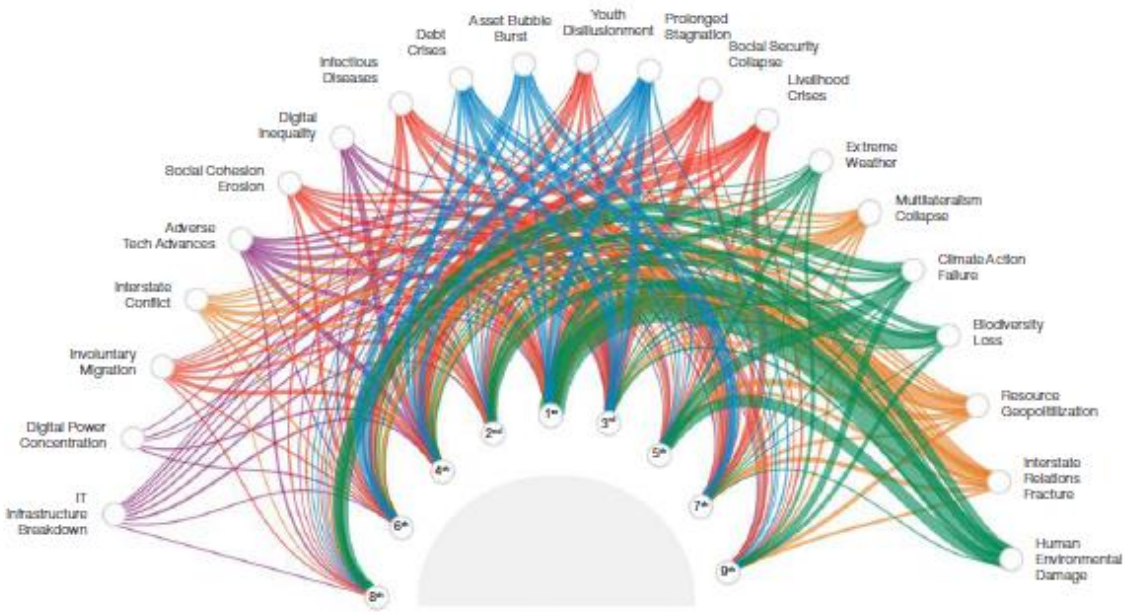
The COSO framework suggests that the first thing to do within a company when it comes to risk assessment is to make sure that the assessment criteria are properly understood across the whole company (Curtis et al. 2012).

Given that a risk can occur due to numerous causes and affect the company's objectives in a variety of ways, the analysis of risks will depend on the availability of data over specific risks, and the resources available to explore that information. Depending on the use intended for the analysis and the context within which it is conducted, the analysis can either be qualitative, quantitative or a combination of both.

Elements taken into account should be, as mentioned above, the likelihood of the risk, meaning the probability of this risk actually occurring, the potential impact this risk could have, should it occur, the characteristics of the consequences; the interconnectedness of the risks identified, the velocity of risks and lastly the effectiveness of the controls implemented to mitigate those risks (ISO, 2018)

While impact and likelihood are widely recognized risk rating scales used in risk analysis, one should bear in mind that the environment companies evolve in has become increasingly interconnected as the economy has globalized. This can be seen in the risk network presented in the World Economic Forum global risk report 2021.

Figure 3: Global Risk Network



Source: World Economic Forum, Global Risk Report, 2021

In this type of environment, dimensions of risk velocity and risk interconnectedness have become increasingly important to take into consideration. Therefore, we will briefly explain those concepts, as well as a proposed methodology from KPMG called Dynamic Risk Assessment.

Risk velocity

According to Quan et al, risk velocity enables company to measure the speed at which the occurrence of an event could impact an organisation. It is defined by the time that has passed between the occurrence of the event, and the moment the first effects are felt by the organisation. It represents an important element to consider when deciding which controls to, implement (Quan et al, 2017).

The COSO framework suggests that being aware of the risk velocity is an asset for developing responses against risks that can be faced (Curtis et al, 2012)

Risk interconnectedness

According to Philbin et al, risk interconnectedness refers to "the analysis that identifies and qualifies the relationships between risks" (Philbin et al, 2013). The author in his report over the increasing presence of risk intelligence highlights two main advantages of taking the risk interconnectedness into account.

First, it enables companies to evaluate the ripple effect a series of small impact risks could have on the achievement of the company's objectives and give them the opportunity to treat them in a timely manner. The report suggests that risks that are highly interconnected should be treated with care in advance, as opposed to more traditional approach where risks are only mitigated when an action comes to be required (Philbin et al, 2013).

Secondly, risk interconnectedness provides companies with information regarding the need to address a risk or simply keep monitoring it. As a result, companies have a better view on how to allocate their resources as having a global view on the network of risks a company is exposed to creates an opportunity to have an integrated plan of action for the risk portfolio of the company (Philbin et al, 2013)

Dynamic risk assessment

In order to implement the dimensions of risk velocity and risk interconnectedness within traditional risk management practices, one of the solutions put forth is the dynamic risk assessment method.

To explain the need for such method, KPMG explains that traditional approach to risk tends to identify risks individually and not take into account the combined effect interconnected risks could have on the company's operations. It is also suggested that companies not taking this dimension onto account face the risk to see their risks spread through the organisation. Having an unifocal view on the risks a company may face does not provide risk management with sufficient data with regards to an optimal allocation of the resources, whereas a dynamic approach as proposed by KPMG would (KPMG, 2019).

KPMG highlights the fact that remaining in a two dimensional-oriented risk management was no longer sufficient for companies to be efficient in the fast changing and globalized world we live in today. Therefore, the consulting firm developed a methodology that combines the dimensions of likelihood, impact, velocity and interconnectedness.

The model uses applied mathematics to analyse data gathered by working with the professionals of the firm that requested the service. A network of risks is then created that allows risk professionals to understand which risks should be prioritized based on the two extra dimensions comprised in the model (KPMG, 2019).

Challenge of risk analysis

Giving a level of importance to a risk is a subjective exercise. Therefore, different perspectives, opinions about the risks faced by a company can arise among the people involved in risk management. Moreover, a risk analysis may differ from one place to another depending on the data used to build the analysis, and the quality of those data. According to the ISO 31000, those limitations to the process should be documented and the decisions maker should be made aware of them. Quantification is also, according to the framework, a difficulty faced by companies in their risk management, and it is suggested that a combination of several measurement methods may provide them with more accurate results (ISO, 2018)

2.3.3 Risk evaluation

Risk evaluation requires an important amount of data to be taken into consideration, and these results are provided by risk analysis as this stage helps companies decide on the most adequate actions to take to mitigate the identified risks, hence the importance of this step in the decision-making processes.

Risk evaluation plays a supporting role in this decision-making process. It consists in a comparison of the data provided by the risk analysis and the characteristics of this risk to decides the measures to implement. These measures may vary according to the evaluation, going from doing nothing, to thinking of control options available to treat the risk, further investigating the risk profile or altering the company's objectives (ISO, 2018).

Results of the evaluation should always be documented and passed on through the different layers of the company to the relevant people.

The COSO Enterprise Risk Management points out the difference between two approaches to the consideration of risks, namely as inherent or residual risks.

Inherent risks are the risks a company faces, as they are if the company did not take any actions against them, that could impact any of the four dimensions defined above (likelihood, impact, velocity, and interconnectedness).

Residual risks, on the other hand, are the risks which remain after the actions have been taken by a company to mitigate them. While this can seem like a straightforward approach, different ways of understanding these concepts can be observed within companies. Some organisations see inherent risks as the events that the company would suffer in case of occurrence, should all their controls fail and residual risks as the impact suffered if all controls are implemented and produced the intended effect.
Other companies, however, consider inherent risks to be the results of the controls already in place, while residual risks would be in this case the risks are treated with the actions planned in case of occurrence (COSO, 2004).

2.3.4 Risk treatment

Treating risks is of course a key element of risk management as this is the step where actions are actually taken to mitigate existing risks. The aim of this step is to make a choice regarding the elements of response to risks the company faces. Risk treatment is an iterative process which involves deciding on the options to use, implementing the risk treatments, evaluating whether or not the actions have been efficient or not, assessing the level of the remaining risk and whether or not further actions should be taken.

Risk treatment choice

Deciding on the risk treatments to implement requires from the companies to weigh the benefits that come from the actions taken against risks, and the costs incurred by the company to implement those actions. The ISO framework notes that risk treatment options are not exclusive to particular risks and should therefore be chosen based on the circumstance in which a risk occurs. Those options can be, for instance, changing strategy to simply avoid the risk, taking the risk, trying to delete the source of the risk, trying to make the outcome of the risk different, altering the likelihood of the risk or even divide the risk between several parties.

Like in any other decision-making process, the opinion of all the stakeholders should be taken into account, as well as the company's prior responsibilities that could interfere with the process. While the economic aspect of the decision at hand is important, it is important to note that the objectives and values of the company should always be considered, as well as the resources the organisation may have at its disposal at this time (ISO, 2018).

It should be understood by companies that all treatments cannot not always have the expected impact. As such, risk treatment is closely linked to monitoring and reviewing processes to make sure to maintain of a level of effectiveness.

Companies should also expect to face situations where no clear treatments stand out, in this case the ISO 31000 suggests organisations to keep the risk concerned under study (ISO, 2018).

In any case, remaining risks should be reported and described to stakeholders of the company.

Risk treatment implementation

The implementation phase of a risk treatment is essential to the effectiveness of the process. For it to be a success, all information related to the treatment plan should be communicated and understood by all the parties concerned so that its success can be controlled. The different steps of the risk treatment should be well understood and integrated within the different layers of the company. Having a well-informed organisation involves several elements. The reasons for choosing a particular treatment plan should be clearly explained and the expected outcomes. Moreover, people holding responsibilities within the plan should be consulted for approbation. The actions required, as well as the resources needed, or alternatives should also be mentioned. Guidelines to allow the plan to be implemented in a timely manner should be part of the information provided to the people of interest (ISO, 2018).

2.3.5 Monitoring and reviewing risk management

Quality of risk management is essential to its effectiveness. Therefore, continuously monitoring and reviewing risk management processes gives assurance to companies with regards to their ongoing activities. Those monitoring and reviewing steps should be assigned to people holding responsibilities for those and the results from this plan of this process should also be clearly defined and planned.

Note that monitoring and reviewing should not be an isolated event in risk management processes, but rather something that should happen all along. Practically speaking, monitoring and reviewing tasks consist of processing data about processes, their results and the feedbacks deriving from the processes. Based on this, actions should be taken to enhance the company's performance and overall processes (ISO, 2018).

KPI's and KRI's

Key performance indicators provide companies with information regarding the level of achievement of the objectives of a company and the effectiveness of its processes. As such, it highlights the areas of improvement a company can work on and see which elements are more critical to consider than others.

In order to select KPI's that are adequate to a company's activities, the organisation should have prior to measurements steps set clear targets to make the measurements possible. Therefore, it is important that the KPI's are updated with the company's objectives (KPI.org, 2021).

According to Alberto G. Alexander, KPI's should be timely, in the sense that they should capture the right information at the right time. They should also be relevant, by using the right data to analyse performance information; critical as they should have a direct link to the organisation's objectives and lastly quantifiable. Indeed, KPI's should give companies a tangible view on the performance of their processes and activities (Alexander, 2021).

KPI's however, only show an image of the state of the business itself and how it's going; "KPIs are simply indicators specifically used to determine how well the company is performing against its business goals" (Parmentier, 2019).

Managing risks being about preventing and mitigating, companies need indicators that can notify them of a coming threat, this is where key risk indicators are essential. According to Alexander, "KRIs are based on warning signs that a company is headed in the wrong direction and could potentially lose value" (Alexander, 2021).

Defining what the right KRI's are can be challenging for companies, but existing sources can guide organisations to find which one would suit their purpose best. In his paper, Alexander explains how companies can use anterior data such as previous incidents, but also internal data such as the risk assessment, the stakeholders' expectations, the strategies and objectives in place, to evaluate which KRI's they should use or not (Alexander, 2021).

Implementing KPI's and KRI's

Implementing effective KPI's and KRI's requires companies to identify and understand the elements of their environment thoroughly. Indeed, the choice of indicators will directly derive from this process and hence, the quality and relevance of the indicators (Alexander, 2021). Indicators should be kept within a reasonable number to ensure the relevancy of all the data it offers. The indications they give should be used to take the adequate measures and align, if necessary, the course of the operations with the company's objectives.

Indicators should frequently be reviewed and dismissed if necessary. Indeed, irrelevant indicators will only bring a biased view of the reality to the company (Lam, 2014)

2.3.6 Recording and reporting risk management

While the primary goal of risk management is to deal with the potential risks a company may face in its activity and how it can affect the company's objectives, recording and reporting risks is an essential step of the process as well. Indeed, making sure that the right information is communicated to the right person in a timely manner is very important to the decision-making process.

To remain efficient, companies should ensure that all relevant e-information is reported in a frequent basis that allows them to keep stakeholders aware of what is happening in the company. Reporting adequately allows risk management to show stakeholders where priorities should stand and hence allows a better consideration of risk management. It also represents an important way to show at the top that risks are being managed properly and how effective it currently is (Ripley, 2021).

Recording and reporting all relevant information related to risk management is a key element of the overall procedure as it is central to decision-making, but also to spread information linked to risk management throughout the company and support exchanges with the different stakeholders of the organisation as this is a key element for a good governance, as mentioned in the governance section. It is also at this stage that the different processes to treat information should be defined based on their level of relevance, sensitivity and potential use (ISO, 2018).

Defining recording and reporting processes will depend on the cost and frequencies of conducting these processes; as well as by the relevance of the information taken into account that will play a central role in the relevance of the decision-making process (ISO, 2018).

Agile methodology

Continuous improvement is a recurring theme within the studied frameworks. As such, we decided to give a short introduction to the agile methodology in order to be able to challenge its use within risk management practices.

According to the Agile Manifesto, the agile methodology follows principles ensuring a fast and continuous delivery of solutions to customers. Note that these principles have been developed to fit the software development environment but have since then been transposed to other fields. This approach allows company to make frequent changes to fit particular requirements and keep performing while developing their project. Therefore, companies produce a competitive advantage through their solution that is continuously sustained. This vision of work implies a strong communication network making sure all relevant information and recommendations are passed on the adequate people (Agile Manifesto, 2022).

The agile manifesto also puts forth the fact that individuals should maintain their skills up to date to be able to help projects evolve in accordance with the requirements and the changes which are requested (Agile Manifesto, 2022).

2.3.7 Technology within risk management

The number of possibilities offered by technological tools in the field of risk management grows exponentially. Those tools, called GRC (Governance, Risk management and Compliance) tooling are meant to support the digitalization of risk management in companies and to automate the processes to ensure a higher level of assurance (Cau, 2013)

According to Racz et al., GRC is "*an integrated, holistic approach to organisation-wide governance, risk and compliance ensuring that an organisation acts ethically correct and in accordance with its risk appetite, internal policies and external regulations through the alignment of strategy, processes, technology and people, thereby improving efficiency and effectiveness*" (Racz et al, 2010).

GRC tools offer companies the possibilities to automate a large part of risk management tasks such as reporting monitoring and making sure that everything that is produced is aligned with the regulatory requirements a firm is subject to. As such, GRC tools help companies align their governance structure and their business goals with their risk management practices (Cau, 2013).

According to Hans Meulmeester, who works as a Technology Director for KPMG Belgium, the use of technology within risk management offers a myriad of possibilities to enhance the productivity of a company as well as its chances to reach its objectives. The automation of these tools allows companies not only to build more assurance as mentioned above, but also to shift the focus of their employees on other core activities which they did not have time for before. Moreover, automated risk management solutions offer cost saving opportunities to the organisations implementing them (Meulmeester, 2022).

According to David Cau, automated GRC tooling is an efficient way to automate the reporting lines and the follow-up processes to make sure all the relevant data is passed on in a timely manner, to the right people and with the right impact (Cau, 2013). The formats of information and the recording of information as requested by regulators is also highly supported by automated tools which take an important workload off the employees' shoulders. Those tools can be adapted quickly in case of regulatory changes since they are constantly reviewed and updated (Meulmeester, 2022).

David Cau sheds the light on the reasons that create the necessity for companies to move towards an automated GRC tooling for their risk management. The first thing mentioned is the fact that the amount of data to cover increases exponentially and more advanced tools are required to process this amount of data efficiently.

Secondly, the fast regulatory changes need to be dealt with fast for companies not to fall behind; automated GRC tooling is therefore an adequate solution to accompany companies in these changes (Cau, 2013).

It should however be noted that all the progress a company can make, depends on its current stage of maturity. As such, companies not yet using any types of tooling should first start to get accustomed to the latter, and once this is done, they should be able to look at automation possibilities within their processes (Meulmeester, 2022).

2.5 Future of risk management: literature review

"Looking into the future", view of the Committee for Sponsored Organizations

According to COSO, the complexity of companies' environment is not to be expected to decrease in the coming years. Therefore, efficient risk management processes will have to be implemented to navigate the uncertainties the organisations will face over the years. Pro-activity towards changes that could be encountered will be, according to COSO, an important element of the years to come for all companies. As such, a more agile way to process risk related data to provide the most adequate answers should be something to aim for among all companies.

COSO highlights several trends regarding what could affect enterprise risk management as we know it. First of all, it is suggested that the amount of data that is being produced is going to force a shift in the analysis are run. This represents an opportunity for companies to use all the data they have at their disposal to operate sound risk management processes. This implies, still according to COSO, that the use of technology should be expected to increase within risk management, especially automation tools and artificial intelligence. In order to justify the cost of risk management, the benefits it provides should be further defined within companies. This will, as suggested by COSO, be supported by the strengthening of the organisational structure of companies where risk management is currently often poorly considered and represented (COSO, 2017).

"Risk Management 2025 and beyond: Priorities and transformation agenda for financial services" by Edwin Star from PWC

Although this report covers financial services, we believe that the areas of interest expressed regarding the future of risk management can be extended to non-financial services as the themes remain broad.

According to Edwina Star, four strong areas should be highlighted regarding the future of risk management: "data and technology investments, sustainable growth, shifting risk profile and lastly integrated risk management" (Star, 2021)

Regarding the future investments in technology, the amount of data to be processed is also mentioned in this report, as well as the necessity to find solutions to comply with the numerous requirements coming from regulators on risk management processes. It is believed that AI-based software and automated solutions will represent a strong asset in the future.

Regarding the sustainable growth, the report highlights the fact that moving towards a proactive way of approaching risk management is going to become a necessity for companies. The author mentions the fact that a shift in mentality will certainly occur by 2025 as the focus will be more on what can be achieved in the future rather than what we can fix from the past.

The report argues, when it comes to the shift in risk profiles, that ESG risks and resilience matters will be treated with more importance in the future given the events encountered during the past years. This is also supported by the increasing size of business networks in which many companies operate.

Lastly, the integration of risk management will be, in the future, a key challenge to enterprise risk management, according to Star. Indeed, the author argues that risk will have to become a core activity within companies in order to have a holistic risk approach (Star, 2021)

"Five objectives for the future of risk management" by Cindy Doe and Amy Gennarini from Ernst and Young.

According to this report, the first challenge companies are going to face will be to embed their business practices with risk management through a clear governance. The authors argue that the approach should shift towards a model where risk provides a global support to other activities. The second challenge put forth by Cindy Doe and Amy Gennarini is the fact that companies should find the right talents to fill their teams. Indeed, it is suggested that one of the keys to the risk management of tomorrow will be to ensure that all the relevant profiles are present in a company's risk management so that all relevant topics are considered adequately.

Moreover, it is suggested that companies should arm themselves with technology capable of harnessing a vast amount of data to be able to take all the relevant information into consideration when setting the risk profile of the organisation. Technology also represents a major challenge as the opportunities companies must automate their processes could allow them to raise their efficiency. Lastly, resilience is expected to be a concern for many companies for the years to come, as it has been proven during the past years as well. Organisations are thus expected to strengthen their reaction capacity against threats that could impact them in anyway and be able to face a crisis, should one occur (Doe et al, 2019).

As a conclusion, one can see that all authors converge towards the idea that risk management should become more integrated within their global operations to create a safer environment for companies to evolve in. Moreover, the idea that risk management should evolve towards technological solutions in order to treat the growing amount of data produced is also an element of interests for the chosen authors.

Those elements are supported by a common vision of a more dynamic expected approach of risk management, as well as by fitted human resources to pursue the required activities

A last element worth noting is the emphasis that was already put on the necessity to be resilient, already in 2019 in the paper produced by Ernst and Young for instance.

Through the research topic explored in the next section, we will try see if the expectations put forth by the authors align with the findings and to what extent the practices observed within surveyed companies align with the frameworks presented earlier in this theoretical section.

3. Practical approach: Risk Transformation Study

As mentioned in the introduction, the practical section of this thesis will be based on a study we conducted during our internship at KPMG Belgium from September 2021 to May 2022.

The Study was conducted in two phases: first a survey was launched to collect data from a broad number of companies active in the non-financial sector (the methodology behind it will be described in the upcoming segment), and secondly the results were processed using Power BI as an analytic tool, to be later discussed during interviews with Partners from each KPMG member firm involved in the Study, namely Belgium, France, Luxembourg, The Netherlands and India, who shall remain confidential considering the report of the Study has not been published to this day.

The insights presented in this section are therefore based on a mix of what came out of the interviews led with these persons and were developed under the supervision of the Risk and Assurance team from KPMG Belgium during our internship. These interviews serve as the sources for the elements developed in the same way they are presented in the report we contributed to during our internship. The interviewees will hereafter be referred to as "interviewed risk management experts"

Through this section, the information gathered will present a fair view on current risk management practices observed in companies today, and how they expect to see their risk management evolve within the next five years. These elements will provide insights on the research topic of this thesis, namely **the challenges and opportunities for risk management in the non-financial sector.**

As the risk management ecosystem of tomorrow is being defined today, this section will bring a common understanding of the current reality and highlight the challenges lying ahead. The main points highlighted from the Study will be explored to help set a clear view on what the risk management of tomorrow could look like.

3.1 Methodology

In order to bring an illustration of the risk management practices confronting the theory presented in the first section of this thesis, a survey was conducted during our internship at KPMG Belgium, as already mentioned. This survey consisted of a quantitative review of the current risk management practices and the expected evolution within the next five years.

The anonymous survey was launched through KPMG in January 2022 and was open for a period of 3 months, until March 2022. Data was gathered from 105 respondents around the world in a closed-ended online questionnaire.

The participating companies were sorted based on a set of defined criteria's such as the industry, the number of Full Time Equivalents, the revenue, the balance sheet figures and the location of their headquarters. The respondents were all active in the risk management sectors, but their level of involvement was not specified.

Our role in this project was central. Indeed, we were tasked with coordinating the process from the beginning until the redaction of the final report. This started by elaborating a question list based on literature we were given by our internship supervisor to inspire ourselves from. The questions we came up with were later discussed and challenged by members of the Risk and Assurance team from KPMG Belgium, before being corrected, when necessary, and finally approved.

Then, we created the online survey and monitored the advancement of the data collection, while most of the invitations to collaborate came from members of the team through their contacts. To reach respondents, the survey was sent out through private emails and via social platforms, the aim being to reach out to a wide range of respondents.

When the survey was closed, we collected all the data from the survey software and drew the first statistical conclusions suing Power BI. We had the opportunity to have discussions with our internship supervisor to highlight the main areas of interest, which eventually led to the interviews topics to be discussed to derive insights from the collected results. Those interviews were planned and executed by ourselves, which was a rich experience from the point of view of an intern. Once all the perspectives from the different interviewees were gathered, we wrote a first report which was later reviewed by members of the team who helped us to make sense of all the data gathered and to come up with the proper phrasing. This part was challenging because even though we had a proper understanding of the topics discussed, we did lack the professional vocabulary to communicate the conclusions the way we intended to.

3.1.1 Building the questionnaire

To determine the relevant questions to ask, the target operating model[2] of KPMG was thoroughly studied in order to point out the areas of interests for the Study. Through an iterative process of brainstorming sessions and workshops with members of the Risk and Assurance team of KPMG, seven sections were selected: Governance, Risk strategy and objectives, Risk identification, Risk management and controls, Risk monitoring and reporting, People and Culture and finally, Technology.

Regarding the questions themselves, it was agreed to have an iterative questionnaire which would allow to study the different patterns among the different respondents. Therefore, each respondent could have different questions coming up depending on their previous answers. The final version of the questionnaire was reached after another series of workshops and reviews in order to make sure all the topics were covered. The question list can be found in Annex II.

The questions were then loaded on KPMG's survey platform. We learnt to use this platform for this occasion, and this helped us to understand how the data would be processed afterwards, but also helped us to develop hard skills in relation to survey creation.

3.1.2 About the respondents

The respondents, although this was an anonymous survey, were asked about the location of their headquarters, the industry they were active in, their total revenues range and the total amount of their balance sheets. This last value was however not retained as a valid source of information as the values were judged to be too close to the values indicated for revenues and therefore deemed to be biased.

[2] The target operating model of KPMG is a guide to transformation for businesses which provides its users with the necessary understanding of what they can achieve by transforming their organization through six components: "Process, People, Service Delivery Model, Technology, Performance Insights and Governance" (KPMG, 2021)

Industries represented and number of companies

Industry	Number of companies
Government	13
Manufacturing	11
Healthcare	9
Services	9
Energy, Oil & Gas	8
Chemical and drugs	5
Transportation	5
Communication and telecommunication	5
Aerospace and defence	5
Real Estate	4
Technology	3
Wholesale and retail	3
Utilities	3
Education	3
Agriculture, forestry and fisheries	3
Others	16

Location of headquarters and number of companies:

Location	Number of companies
Belgium	46
France	32
Netherlands	8
Luxembourg	8
Germany	2
Europe (excluding Belgium, France, Netherlands, Luxembourg and Germany)	1
Outside of Europe	8

Distribution of employees and number of companies:

Total number of Full Time Equivalents	Number of companies
0 – 100	7
100 – 500	10
500 – 1000	6
1000 – 5000	37
5000 – 10.000	20
Over 10.000	25

Distribution of revenues and number of companies:

Revenue size	Number of companies
Less than €100 Million	14
€100 Million - €300 Million	8
€300 Million - €500 Million	13
€500 Million - €1 Billion	17
€1 Billion - €5 Billion	27
€5 Billion - €10 Billion	9
€10 Billion - €30 Billion	11
Over €30 Billion	6

3.1.3 Limits of the survey

Several limits were highlighted as the results of the survey were processed. The first one we would like to mention is the fact that no tangible proof of the level of expertise of the respondents was gathered. The validity of the answers gathered is therefore based on the honesty of the people who took the questionnaire as it was stipulated in the various reach-out messages that they should be active in risk management in order to answer. In order to remediate this, the survey could have been pointed directly at specific people with specific profiles, but this would have made it difficult to raise a large number of answers.

The second limit we would like to highlight is the length of the questionnaire. Indeed, there were a total of 102 questions which was deemed to be long for a large number of companies.

More than 400 respondents opened and begun answering the online survey, but the statistics showed that only 1 out of 4 respondents had completed the questionnaire, although they had the possibility to anonymously save their questionnaire and finish it later on. Though no direct solution can be found as all the questions were deemed to be relevant to cover all the topics, better explaining the length of the survey and the options the respondents had to complete it could have been a good way to retain more respondents

Lastly, we noted that the different categories represented were not equally distributed. To obtain more relevant results, it would have been interesting to even the population out so that direct comparisons could have been made.

3.2 Results analysis

3.2.1 Governance

The increasing expectations towards corporate governance due to the everchanging complex risk landscape, triggers Boards of many organisations to re-evaluate the effectiveness of their governance frameworks.

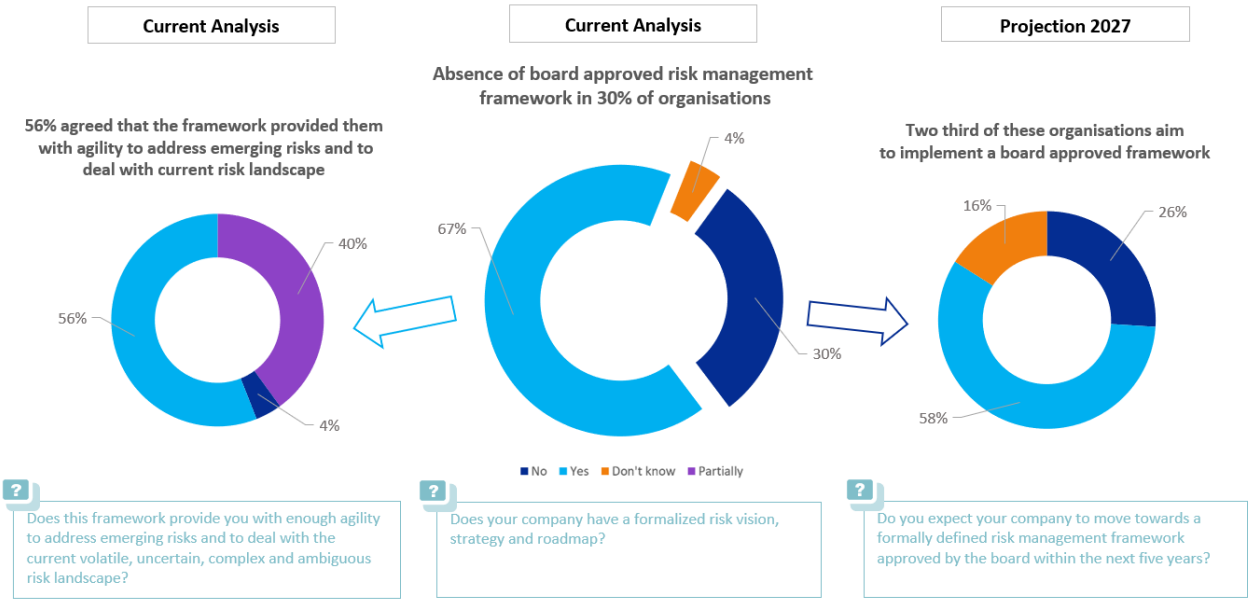
The Study focused on the existence and formalisation of the governance and risk framework and its agility to deal with the future uncertain and complex risk landscape. The Study questions were articulated around the composition, expertise and role of risk committees and risk functions to gain more perspective on this committees. Collaboration between the lines of defence is a key factor for an efficient risk framework and this topic was also covered extensively in the survey.

The combination of risk management and business continuity equips organisations with business resiliency to address uncertainty and promote stability. The importance of the business continuity and crisis management framework within the organisation was scrutinized.

The perceived evolution of all the above-mentioned governance and risk aspects were explored over a five-year period to forecast changes and trends.

Integrating governance and risk

The survey revealed that the risk management framework was not formalised by the Board for 30% of the companies. This raises the question of how risk management activities are handled from a general perspective for these organisations.



Many organisations realized that they needed to be on the front foot of risk, and this is feasible when the risk management framework is embraced from the Board to the front line. 58% of the organisations without a formalised risk management framework intends to implement one in the future.

When the Board is not involved in the conception of a risk management framework, it can raise questions about the decision taking powers of the Board and the elements considered to make those decisions.

According to the interviewed risk management experts, governance structures are the basic foundations of an organisation. This includes the involvement of senior management to ensure a proper flow of information and instruction to ensure a common direction across the layers of the organisation and a sound decision-making process at the Board level. A strong governance structure and therefore a formalised risk management approved by the Board is a highly valuable asset, as it brings an important support to the integration of risk management activities across the different layers of the organisation. This in turn translates to clear messages and actions which, once reported to the senior management level, can bring meaningful insights to allow coherent decision making in turn.

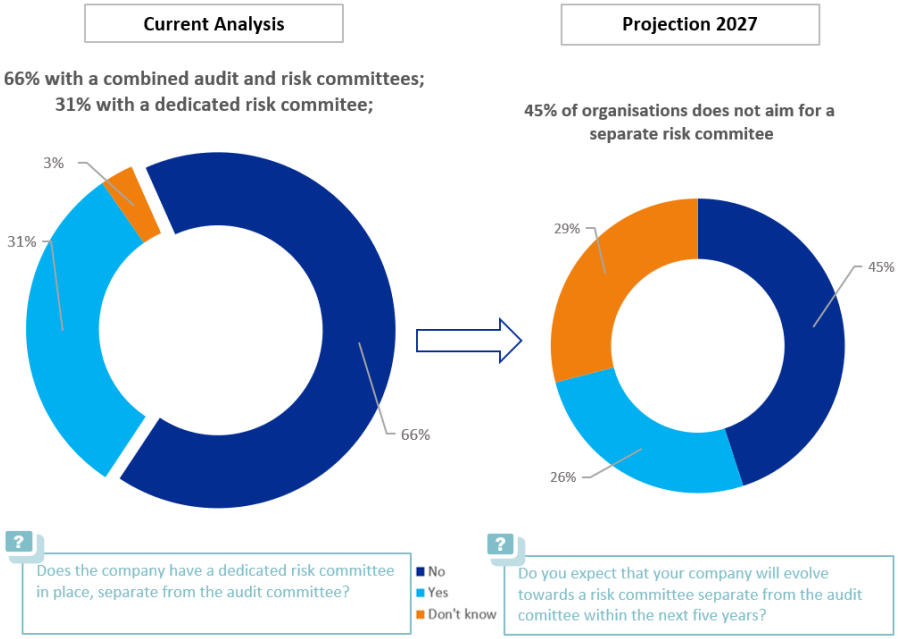
Companies developing or reviewing their governance structure have the possibility to consult the local code of corporate governance as a reference for best practices whereas best practices for the risk framework can be consulted within the COSO framework or the ISO 31000 framework.

On the compliance side, organisations should constantly monitor new legislations, their corresponding compliance requirements, and impact on their risk management framework. Even though regulations with respect to risk management are still very limited for the non-financial sector compared to the financial sector where there are numerous regulatory requirements and compliance occupies an important role in the integrated Governance Risk and Compliance (GRC) model, a constant monitoring of upcoming regulation will give companies the opportunity to adapt ahead of time.

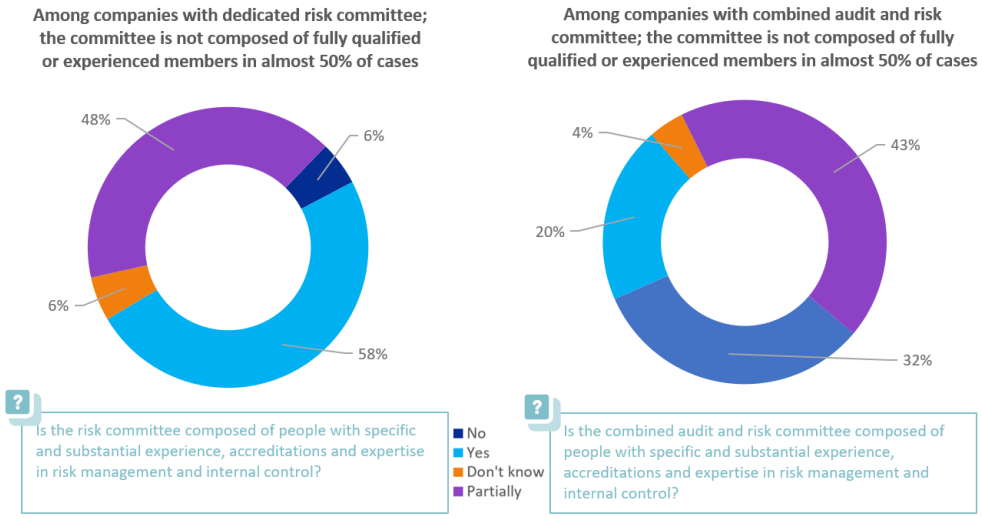
Upskilling the audit committee

The Study revealed that two thirds of the companies surveyed did not have a risk committee separate from their audit committee.

66% of the companies displayed a combined audit and risk committee. Among companies with a combined audit and risk committees, half of them do not foresee a separate risk committee in the next five years.



Overall, almost half of the companies declared that their committees were partially made up of qualified individuals with specific and substantial experience, accreditation (such as ISO 31000, CIA or equivalent) and expertise in risk management and internal control regardless of the nature of their committee. It was however observed that the presence of individuals qualified in risk-related matters was more important in separate risk committees than in combined audit and risk committees.



Risk management oversight functions require specific expertise and skills to ensure proper consideration to risk-related subjects. Not having a fully qualified or experienced committee poses an important challenge to organisations as it undermines the effectiveness of the oversight role and can lead to difficulties to challenge arguments on risk management. Moreover, an inadequate composition of the committees can lead to omissions of topics or unfounded discussions.

According to interviewed risk management experts, having adequately composed risk committees with members with the right balance between a thorough knowledge of the company's situation and a strong knowledge of risk is a strong asset for companies. Indeed, a committee with a complete set of knowledge and skills will bring an added value to the company by ensuring all relevant matters are discussed and later on transposed in decisions and actions. These committees represent a key point in the flow of information and the potential they offer should not be disregarded.

In order to be effective, risk oversight should be supported by people with strong knowledge and background in fields related to risk to make up the separate risk committee or combined audit and risk committee.

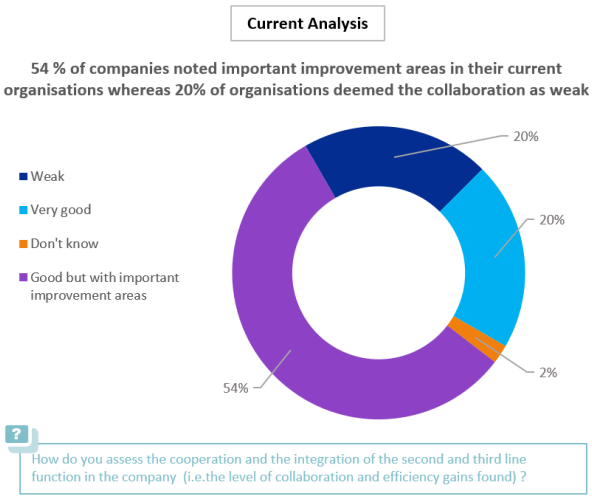
Indeed, more finance-oriented experts do not have, in many cases, the required knowledge on risk operations in other fields than their own. In both cases (separate or combined committee), the main goal is to keep the Board informed regarding risk-related topics; and this is very important as it is the Board who remains accountable for the decisions taken by the company and therefore, its performance (KPMG, 2021).

Whichever committee takes the lead, their aim remains to facilitate focused and informed Board discussions on risk-related matters. It is the Board who retains ultimate accountability for the adequacy and effectiveness of the organisation's risk management arrangements.

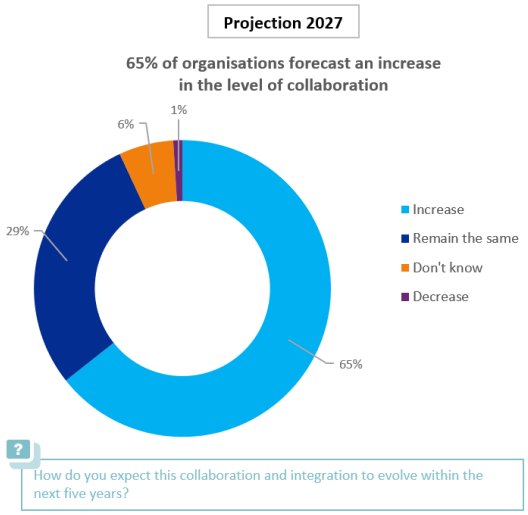
Outlook at the three lines of defence

"The Three Lines Model has largely been viewed as the basis for sound risk management," as quoted by the IIA President and CEO Richard Chambers (2020)

According to 74 % of the companies, the collaboration between the second and third lines of defence are insufficient and 65% of the organisations perceive a shift towards more collaboration between the two lines of defence in the future.



A lack of collaboration between the second and third lines of defence does not only lead to duplication of efforts, but also to incongruous language used by those two functions, resulting in a diffused message to senior management. This kind of silo approach reduces the importance and focus of risk management activities.



The challenge is therefore not only to build a coherent communication channel between those two lines and to the senior management, but also to ensure the recognition of the added value this system has to offer. Setting up these elements represents an opportunity to provide risk management with more recognition within governing organs, giving risk professionals a stronger foundation to work on.

According to the interviewed risk management experts, the efficiency of the three lines model lies within the definition of each lines' responsibilities and understanding of their respective scope of action. Improving the collaboration between the second and third lines of defence therefore starts with the two functions understanding each other's responsibilities and duties. They should also communicate on their ongoing projects and results to avoid duplication of efforts due to lack of exchanges, as mentioned above, but also to keep their risk cartography continuously up to date. Companies developing or reviewing their governance structure are advised to consult the local code of corporate governance as a reference for best practices whereas best practices for the risk framework can be consulted within the COSO framework or the ISO 31000 framework.

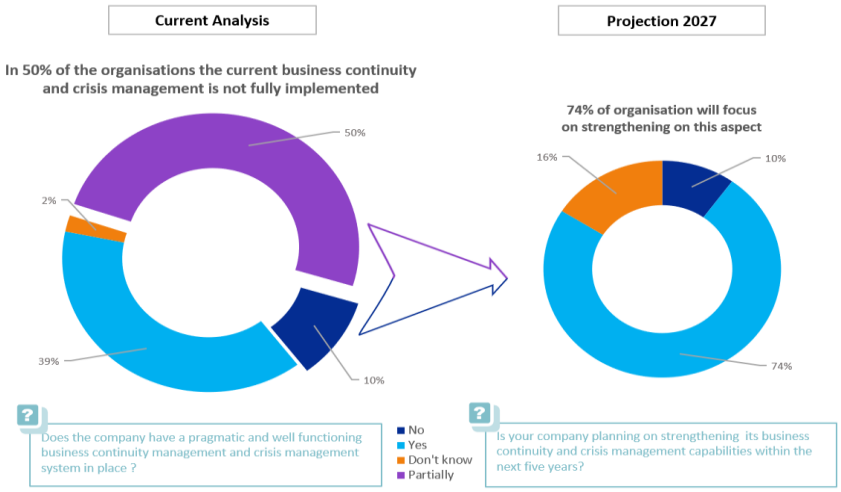
The first line officers are the ones that practically deal with the risks directly and should be given due importance. It is important that the first line considers the second one as a function of support, and not as an oversight function playing the role of a regulator. The role of the second line of defence is often mistakenly believed to be the one managing the risks, whereas it should pose as a facilitating line for the first line, which is the one managing risks the company faces. Collaboration and confidence between the first and the second line are equally important to ensure that the system operates smoothly as it creates the opportunity to run soundly the operations.

A forum for the three lines of defence can prove to be an efficient way to align their tasks and responsibilities to allow them to work in an efficient way, but also to deliver a clear message to senior management, which is again an opportunity companies could benefit from.

Expecting the unexpected

Despite the unprecedented events companies faced during the previous years such as the Covid-19 outbreak and the current situation with the war in Ukraine, it was pointed out that 50% of the companies surveyed did not yet have a fully pragmatic and well-functioning business continuity management and crisis management system.

Threats can cause disruption or even business failure if not addressed effectively and a Business Continuity Management System can make the organisation incident proof. A well thought framework to deal with incidents can lead to an effective response and a quicker recovery.



Although, 70% of the companies concerned revealed that they aimed to invest on business continuity plan and crisis management. Changing the approach from a reactive to a proactive one will enable the organisation to face any unforeseen situation, event or crisis.

Following the interviews with risk management experts, it is suggested that the active involvement of the Board is essential to integrate reliance within the overall strategy of the organisation. Building Business Resilience does not only represent an opportunity for companies to be able to remain viable, evolve and thrive, but it is also a way to build an alternative view on how the business can function (KPMG, 2020).

Analysis of the current crisis management in most organisations revealed that they are based on static business continuity plans which are not always easy to apply and use in practice. In addition, many people within an organisation are not always aware of their roles and responsibilities.

It is therefore recommended that organisations implement a crisis management framework adapted to the specific situation they are facing consisting of practical tools, templates and checklists that is continuously updated and involves the entire organisation.

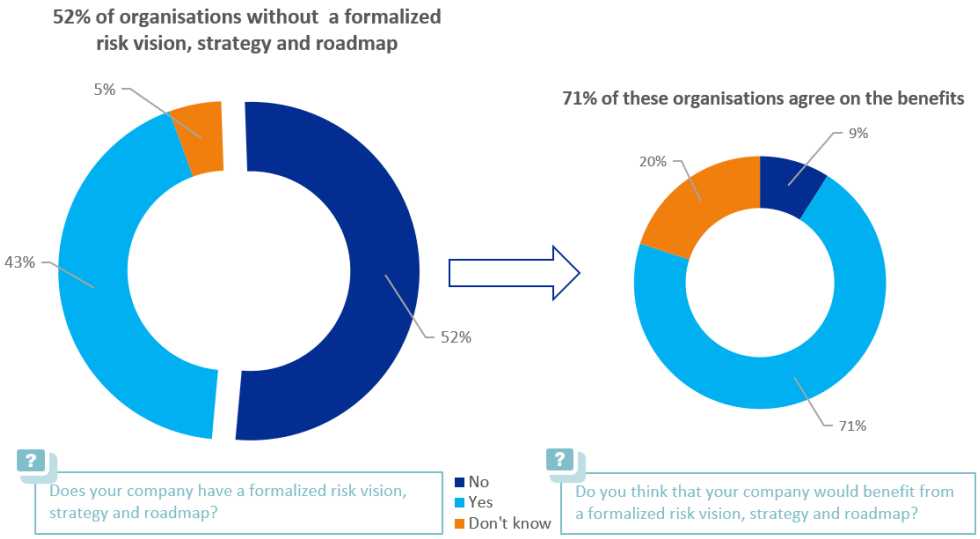
3.2.2 Risk strategy and objectives

Aligning vision and strategy is a key element of successful risk management framework. The focus of the Study was to enlighten on the existence, awareness and alignment of the risk vision, strategy and roadmap. Another important aspect investigated was the inclusion of risk management within the strategic and decision-making process of the organisation and whether a risk appetite framework was defined and implemented. Performance monitoring and reporting provides transparency and ensures continuous improvement and thus the emphasis was placed on the existence of the types of metrics in place to monitor risk performance as well as the reporting mechanism. Finally, the link between the outcome of risk evaluation and renumeration was considered.

Envisioning risk management

According to Professor Christophe Lejeune (2021), it is essential for companies to have a clear vision aligned with their strategy to achieve success. The vision should be in line with the company's global objectives and be used as a guideline for the way the company should exist. Strategy should clearly state the way the company should evolve depending on the events it faces and lastly, the design and roadmap should show how the two first elements can articulate within the company's expectations for its project (Lejeune, 2021).

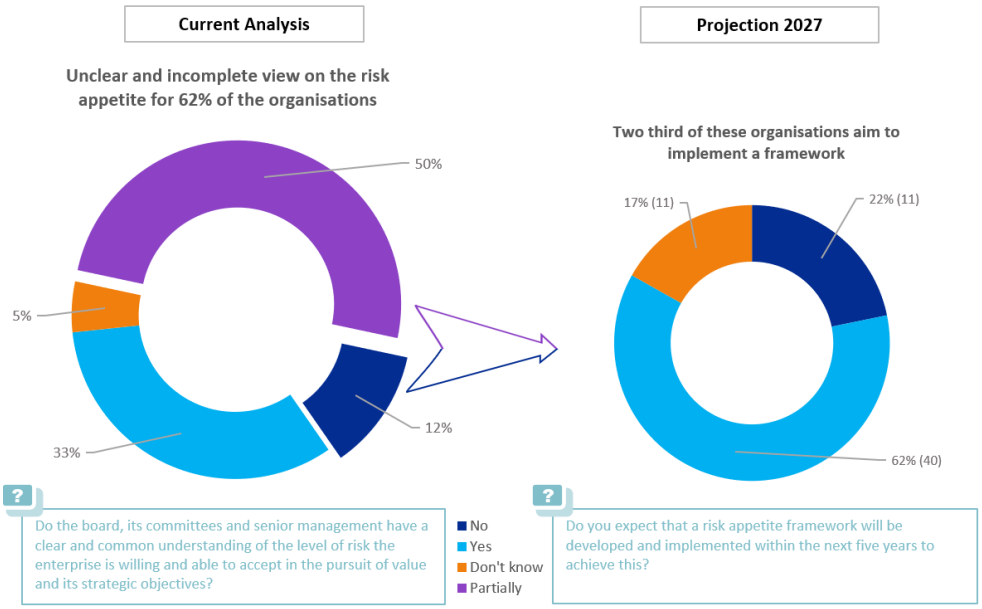
Remarkably, 52% of the companies did not have a formalised risk vision, strategy and roadmap with regards to risk management, although almost three quarter of the same companies agreed that they would benefit from a formalised risk vision, strategy and roadmap.



Setting the risk appetite

62% of the respondents highlighted that their Board, committees and senior management did not fully understand the level of risk the enterprise was willing and able to accept to pursue its strategic objectives. Implementing a risk appetite framework could be an opportunity to address the problem and is supported by the fact that two third of these companies expect to develop and implement a risk appetite framework in the future.

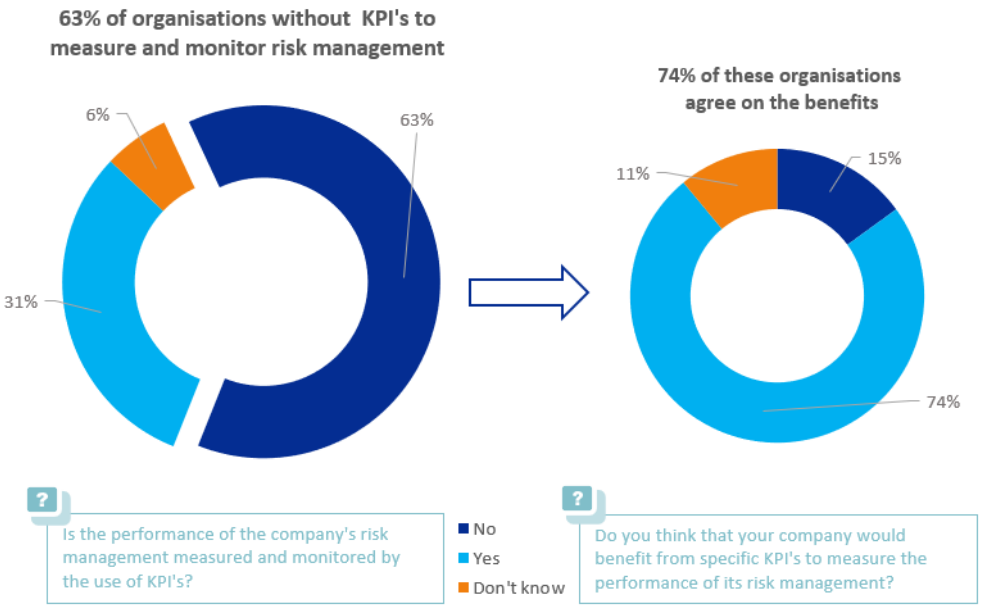
According to the interviewed risk management experts, many executives seem to believe that the organisation's risk appetite can be intuitively defined. The challenge is therefore creating a common understanding of the risk appetite among the Board and executive team due to the subjectivity associated with it.



When used strategically, it is suggested that risk appetite frameworks can strongly help organisations to align the strategic objectives of the company with the performance expected by the organisation's stakeholders. According to KPMG, risk appetite can be a strong asset for businesses to take the measure of the risks the company can take within the decision-making processes. Its purpose is to help firms figure whether they agree with their position on the risk spectrum, which goes from high tolerance to risk, to low tolerance. Operating without a risk appetite framework, however, makes it challenging for companies to understand where they stand on this risk spectrum and therefore exposes them to being confronted to too few or too many risks, both of which can be unhealthy for a business. The lack of consistency will be reflected in the strategic and decision-making processes (KPMG, 2013).

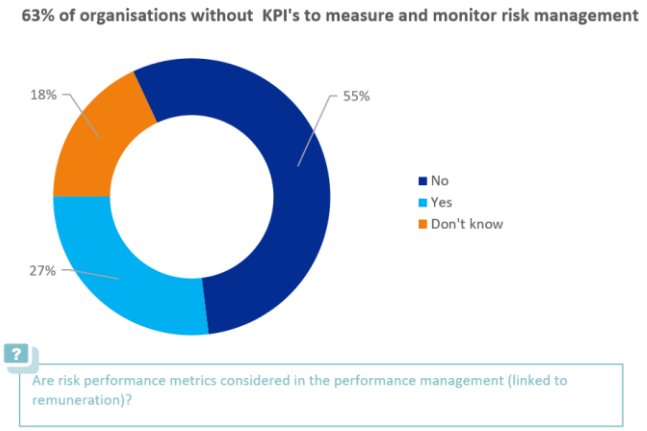
Challenging performance

KPI's are not implemented in 63% of the sampled population though three quarter of these businesses agree on the benefit of using them to measure and monitor risk management performance.



It was understood from the interviews with the risk management experts that one of the main difficulties for these companies was knowing what they wanted to measure and knowing the relevant benchmark to confront their measurements to.

From the survey statistics, it can be noted that 55% of companies are not using tools such as risk metrics to review their employees' performance and hence not benefiting from the added value it could bring.



A common understanding and approach regarding vision, strategy and roadmap is an opportunity for companies to integrate the various components of their risk management in the organisation's bigger picture. Moving towards such a model should translate into aligned actions from each layer of the company, with a common direction

To fully address the numerous challenges faced, companies should define their risk appetite, understand and identifies what needs to be measured. This will in turn help them define what indicators or tool would best suit their needs and will offer them the most relevant results.

Once the measures identified have been implemented, they could benefit from a continuous improvement cycle for risk management, through measurement of the performance of an activity or people, continuous development of people and a strengthening of the risk culture through the incentives to meet the objectives.

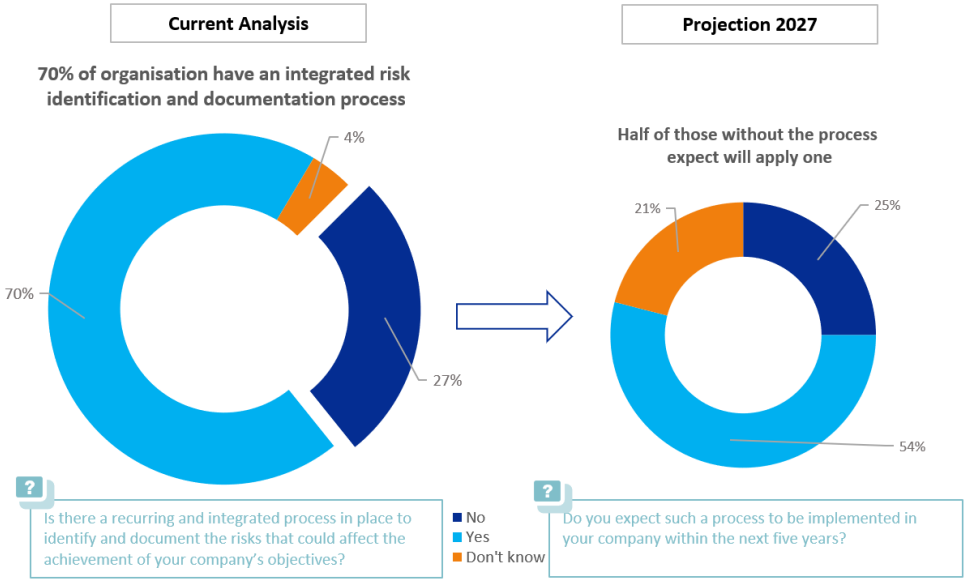
3.2.3 Risk identification

In these times of uncertainty, companies are expected to approach risk assessment through new eyes and more innovative solutions. The objective of the Study in this section was to review whether a strategic and coordinated approach to risk was in place. The current risk identification was analysed with regards to types of risks identified, the frequency of the identification process and the data referred to in the process.

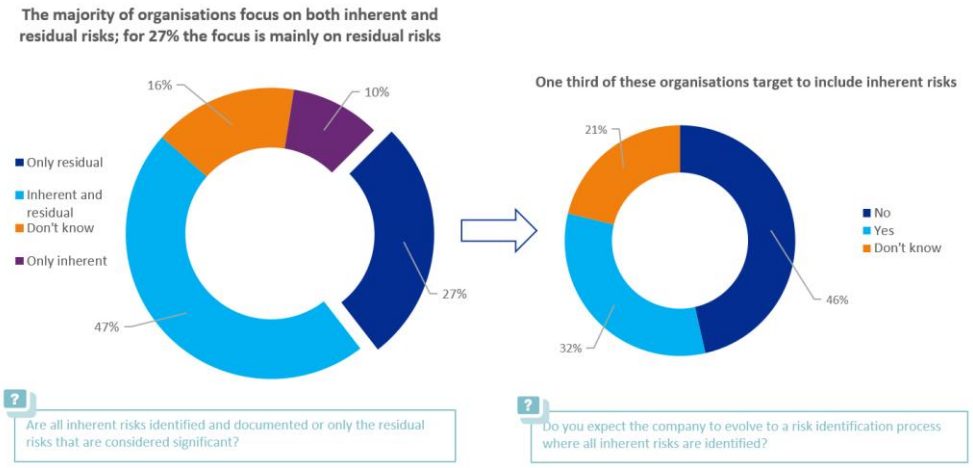
Focusing on the right risks

Two third of the companies with an existing risk management framework agreed that the framework was agile enough to address emerging risks and to deal with the current volatile, uncertain, complex and ambiguous risk landscape.

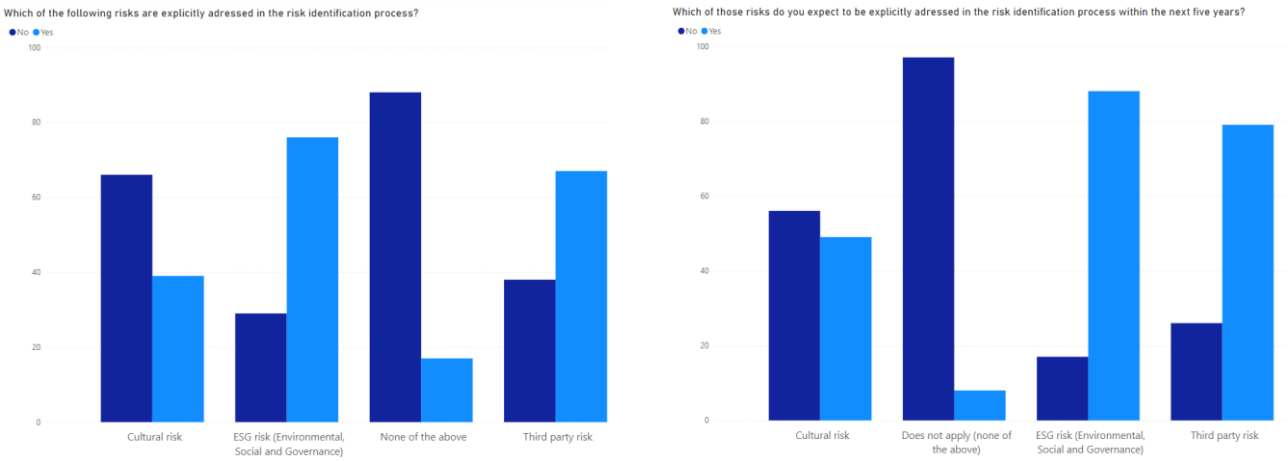
70% of enterprises affirmed the existence of an integrated process to identify risks and half of the organisations without one, aimed to implement a similar process in the future.



10% of the companies focused on inherent risks only whereas and 27% focused on residual risks only. 1 out of 2 of the organisations measuring only residual risk were not convinced of the utility to measure inherent risks in the future.

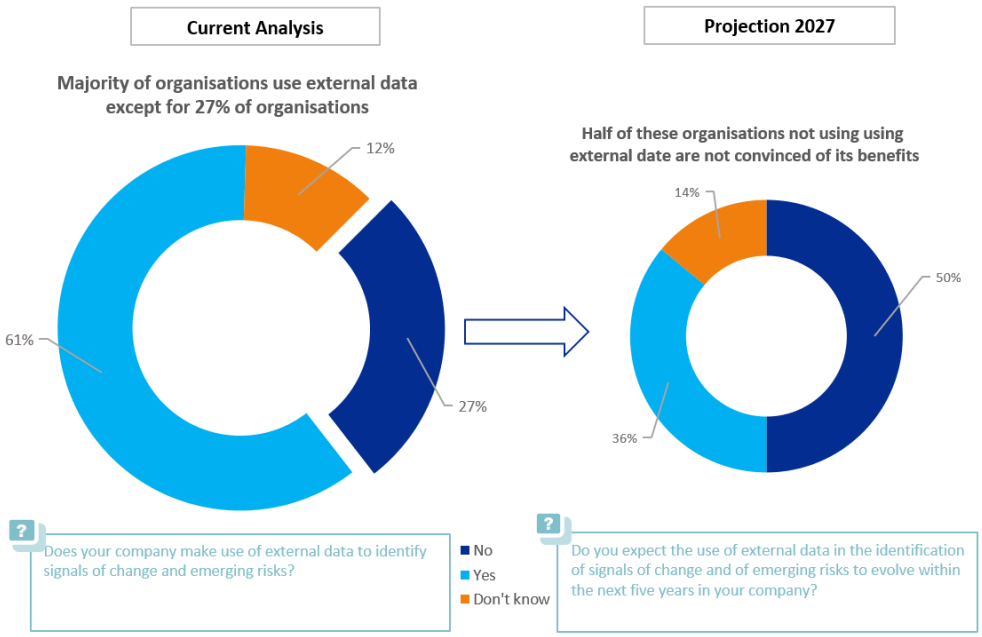


It was noted that considerate attention was paid to emerging risks such as Environmental, Social and Governance risks and third-party risks, which is reflecting the predictions described in the theoretical section.



The ISO 31000: Risk management (2018) framework suggests that companies have access to the “best available data” when managing their risks.

In most cases, reference is made to external data for risk identification process except for 27% of the companies. Surprisingly, only a third of these organisations, are convinced to use external data in the future.



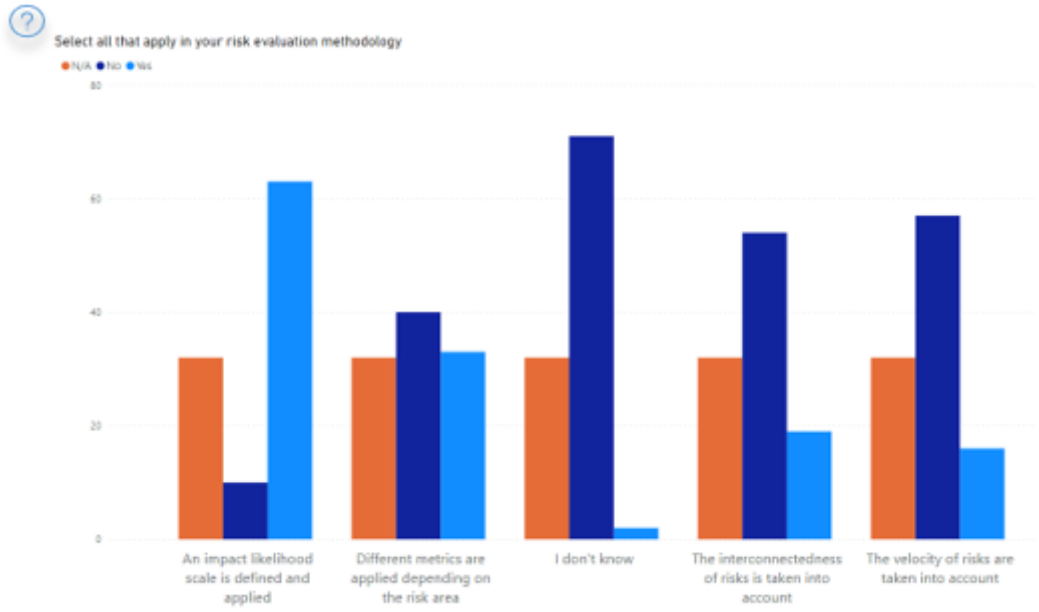
Neglecting external data can make it complicated for these companies to identify trends and to proactively include them in the risk cartography. Indeed, external data provides another perspective on the risks the organisation can encounter and complete the source material at the disposal of the company for the purpose of risk identification. Interviewed risk management experts suggest main challenge with external data is to know which external information is relevant and on which platforms to have access to this information.

3.2.4 Risk management and controls

Risk assessments are evolving to help people and organisations better understand the complex world they live in and future risk scenarios. In this section, the emphasis of the Study was on the evolution of risk assessment methods, risk treatment strategies and the internal control framework to manage and monitor internal controls.

Globalizing the approach

Risk assessment is a complex and challenging process and failing to identify a risk can be consequential for the organisation. A large proportion of organisations might find themselves in this challenging situation as only 10 % companies surveyed included both risk interconnectedness and risk velocity within their risk assessment. Adapting their risk assessment models represents a true opportunity for companies as the only dimensions of impact and likelihood are not sufficient to keep up to speed with risks.



According to the interviewed risk management experts, this approach elevates risk management from a static and basic 'must-do' exercise a more globalized and dynamic exercise including other new dimensions such as risk velocity, risk interconnectedness or any other relevant dimensions. Organisations incorporating this approach within their current framework will require the development of capabilities.

Given the complexity of the process and the specific skills required, these organisations may require the services of an external service provider.

Utility of dynamic risk assessment

As explained in the theory section of this thesis, Dynamic Risk Management is an approach which represents an opportunity for companies that use it with respect to risk identification. Indeed, the precise scientific and mathematics foundation behind it allows companies to consider dimensions of risk interconnectedness and risk velocity to provide a clear risk profile of the organisation. This method therefore allows companies to determine where contagion can be expected between conventionally isolated risks.

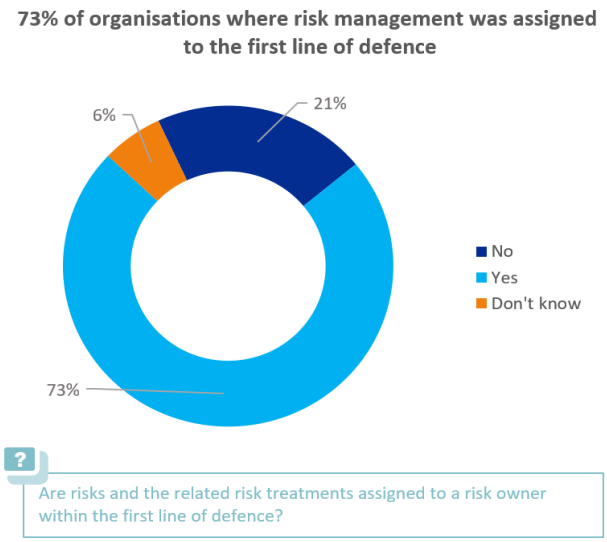
It uses network theory and proven scientific methods to determine whether individual risks to a business can be expected to cluster together (interconnect) to form concentrations of risk events, and to determine where there is expected contagion between structural breaks and organisationally idiosyncratic risks (KPMG, 2020).

Recent events and changes in the global economy proved that organisations which fail to adapt could be impacted with the risks that they previously rated as non-critical based on their likelihood.

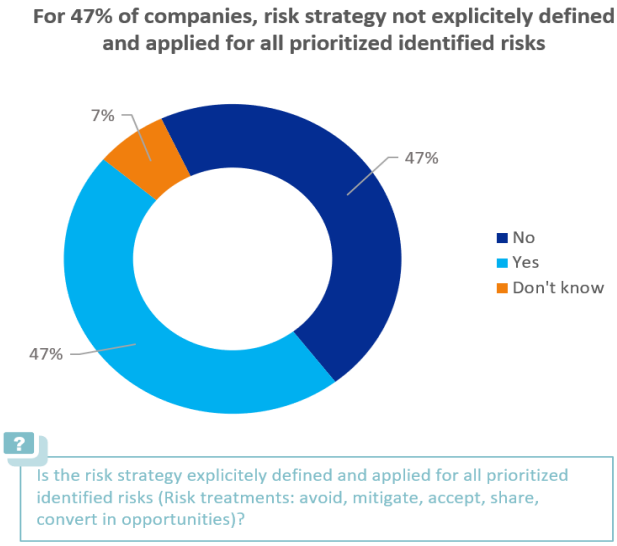
Although the same risks could be anticipated if velocity and interconnection with other risks were considered.

Actioning the strategy

The first line officers are the ones that practically deal with the risks directly and should be given due importance. This was observed in 73% of cases whereby risk management was assigned to the first line of defence.



It is worth highlighting that 47% of the companies did not consider their risk strategy to be explicitly defined and applied for all prioritized risks.



Interviewed risk management expert suggest that governance should set the tone for risk management strategies to be translated into actual actions to build a strong control system. Alignment between the lines of defence is a challenge as it ensures the correct strategies are implemented and hence ensures an efficient risk management system.

An appropriate risk strategy is easier to define when the risk owner has a deep understanding of the risk. Another reason for risk strategies not being applied is the lack of coordination and alignment between the lines of defence. The actions that should normally derive from the strategy are often not reflected in the actions taken by first line officers, due to a lack of understanding or a lack of communication with the second line of defence.

Understanding the internal control system

The implementation or existence of an Internal Control Framework approved by the Board is a mandatory requirement for listed companies and a recommendation for non-listed companies by the local Code of Corporate Governance of several countries.

Despite the recommendations of the code, 40% of the surveyed companies lacked an internal control framework to manage and monitor key controls. As the interviewed risk management experts put it, the absence of a formalised internal control framework poses a real challenge for organisations to remain efficient and relevant in the way they treat their controls.

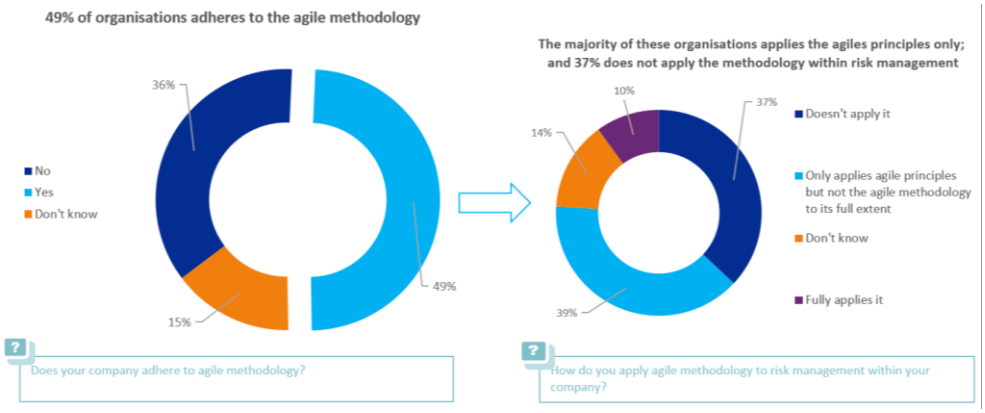
As the code adopts the 'comply or explain' approach, these companies are not compliant with the code and are not able to explain their internal control system. Even organisations with an existing internal control framework can face difficulties to explain their internal control framework which can lead to lower assurance for control activities, and again to duplication of effort and inefficiencies.

To ensure standardization in operations, it is essential to understand the system within which controls are managed. Organisations have the possibility to refer to their respective code of corporate governance for guidance around the principles and best practices that their internal control framework should follow and to enquire on how to set it up as this is one of the most challenging parts of the process.

Building up agility

Agility is the foundation of innovation and has been proven to support growth in organisations operating in highly dynamic environments. The Study reviewed the extent to which the agile principles and methodology were implemented in the surveyed organisations.

The survey results pointed out that 49% of the surveyed companies adhered to the methodology, meanwhile when questioned further it was highlighted that only 10% fully applied the methodology, implying that the other respondents only adhered to the agile principles without applying them within risk management.



Despite the uncertainty surrounding the future use of agile methodology within risk management, a third of the respondents believed the application of the methodology will remain static, on the contrary a quarter believed that the trend would be a move towards the application of a fully agile methodology.

Considering the agile methodology basics and risk management activities, interviewed risk management professionals consider that it can be justified that many companies do not apply the methodology as in most cases risk management activities are neither considered as projects, nor deemed as a complex process. Companies should however contemplate on the added value that the agile methodology can bring within their risk management framework as an opportunity to embrace in the future. Indeed, following the agile methodology gives firms the possibility to quickly adapt the parts of their risk management framework based on new trends or inefficiencies, hence allowing them to keep all the positive aspects and only improving the aspects that need to be enhanced.

Adopting a proactive and dynamic approach to continuously deal with emerging trends will prevent organisations from being negatively impacted by a risk, which may not be the case of companies that adopt reactive postures towards the risks they encounter. As a starting point, companies could define how agile methodology is relevant within their business environment. Further to this exercise, the agile principles stated by the agile manifesto should be transposed into actions that suit risk management activities.

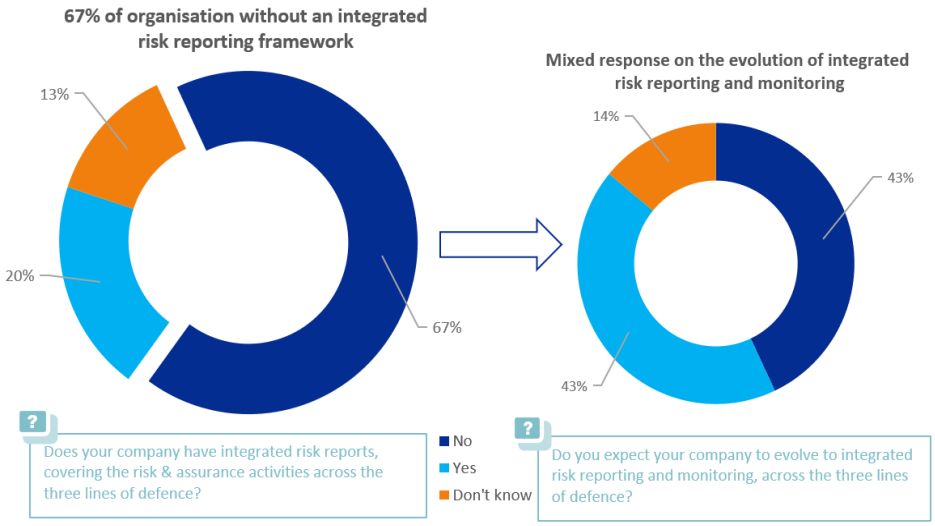
3.2.5 Risk monitoring and reporting

Risk monitoring and reporting is one of the main pain points faced by many organisations. COSO has highlighted the importance of risk reporting in its COSO ERM Framework as "reporting supports personnel at all levels to understand the relationships between risk, culture, and performance and to improve decision making in strategy and objective setting, governance and day-to-day operations." (COSO, 2017)

Integrating the reporting

Addressing risks in isolation can often seem like a solution for companies but adopting a strategic and coordinated approach to risk allows organisations to better integrate data and therefore improve risk management efficiency.

There was no integrated risk reporting framework in 67% of the surveyed companies and this originates from the absence of an integrated risk management framework tackled in the segment covering Governance.



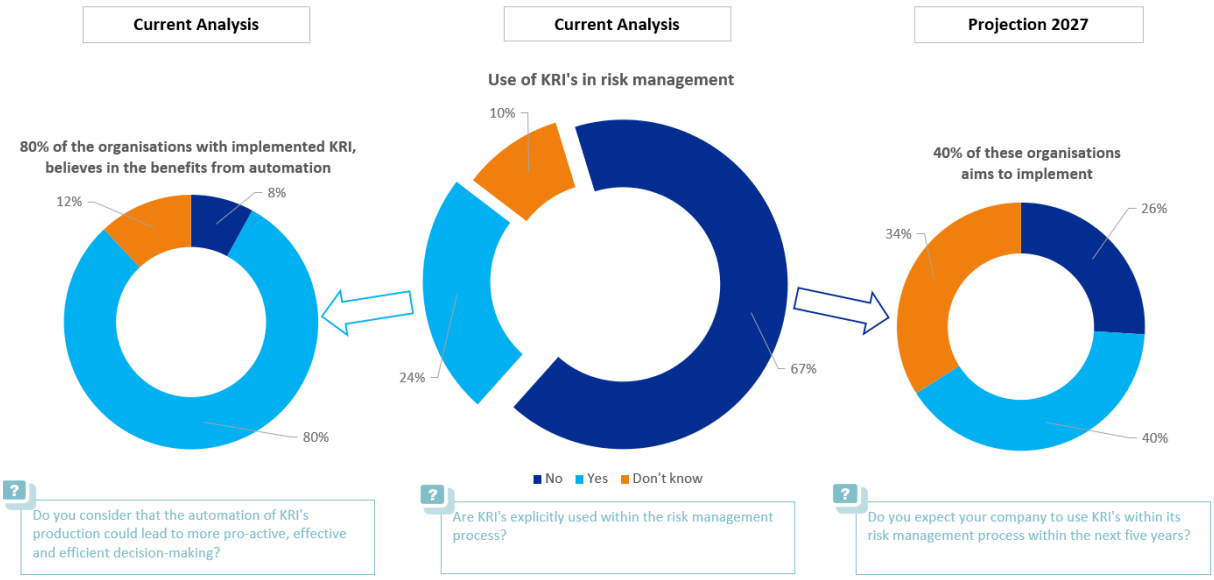
According to the interviewed risk management experts, unclear information within risk reporting can result in inconsistent information reported in a diffused manner across the different layers of the company. The clarity needed for risk management is often blurred by silo views offered to governance bodies, which is a challenge as it does not leave room for a considerate decision-making process. The root of this issue therefore partly lies within the fact that not using integrated reports makes it very challenging to show the reality at the top. The picture shared with decision-makers is not an exact reflection of the reality and does not have the intended impact in terms of actions taken.

Integrated risk reports could however be a great opportunity for organisations by helping them to build strong synergies within the risk management activities. Collaboration between the different actors will support the coordination of actions and will provide governing organs with clear, coherent data which will give an added value to the information and will in turn provide companies with a decision-making process that is complete and well advised. Decision makers will be more inclined to listen to what risk management has to say if the message is aligned and distributed through a common channel and format that includes all the required elements.

Automating KRI's

The level of risk can be continuously measured through a series of defined indicators and the potential of these indicators are not identified or exploited in 67% of the surveyed companies. The use of KRI's facilitates the process to identify new trends so that they can be dealt with on a timely basis.

The forecast that KRI will be adopted in 40% of the organisations by 2027. As mentioned earlier, a dynamic approach is one of the main factors that will reinforce the existing risk management framework. One of the actions contributing to the reinforcement will be the identification and implementation of KRI.



Quantifying KRI's represents a challenging step for many organisations due to the subjectivity surrounding the selection of indicators. One important step is to understand and define what companies want to measure before setting up indicators.

4 out of 5 companies which use KRI's believed that the future of KRI's lies in automation for the main reason that it increases the assurance level with respect to the quality of the information. On the other hand, it will also be an opportunity to standardize the process and thus minimize or erode the associated subjectivity. This can be easily achieved through the implementation of adequate tooling.

According to Hans Meulmeester (2022), GRC tooling can be an efficient solution to standardize the quantification of risks to create a more pragmatic approach that risk professionals can rely on. Data analytics will play an important role in this challenge, it is therefore important that companies consider the use of data analytics based on their current maturity levels. Applying this type of solution will allow organisations to get the best out of available data once companies learn to explore its possibilities and they can use it to derive maximum benefit. The functionalities of the GRC tooling capabilities and benefits will be addressed in the Technology section of this thesis.

Clarifying and communicating reporting protocols

The survey shows that 50% of surveyed organisations does not have embedded reporting and escalation protocols within risk management. In many situations, when there is a lack of systematic reporting, there is no clarity over who does what and when should it be reported when there is a problem. These inefficiencies can lead to companies being overwhelmed by their risks and not being able to mitigate them as they should have, because information was not passed on properly.

A solution to this issue which is put forth by the interviewed risk management experts is the use of dashboards, which allows companies to have a view on a summary of risks and their controls, which eventually lets users efficiently identify key areas of interest and perform thorough analysis of the relevant data. Opting for a dashboarding solution for reporting matters therefore represents an opportunity for organisations to enhance their efficiency and effectiveness by clarifying the reporting information.

Clear reporting lines should be communicated, and it should be ensured that the relevant information is always reported to senior management who will decide on the action based on the events observed.

Another reason that could explain the results presented hereabove might be the absence of mechanisms or tools to measure and report risks. Indeed, according to the interviewees, this might not be a pressing matter at the initiation of the risk management process, the growing scale of risk assessment as the business expands and the increased complexity of risk data gathered overtime may lead to a situation where traditional reporting may not be an ideal approach due to the challenges posed the gathering and the visualisation of all the risk data.

3.2.6 People and culture

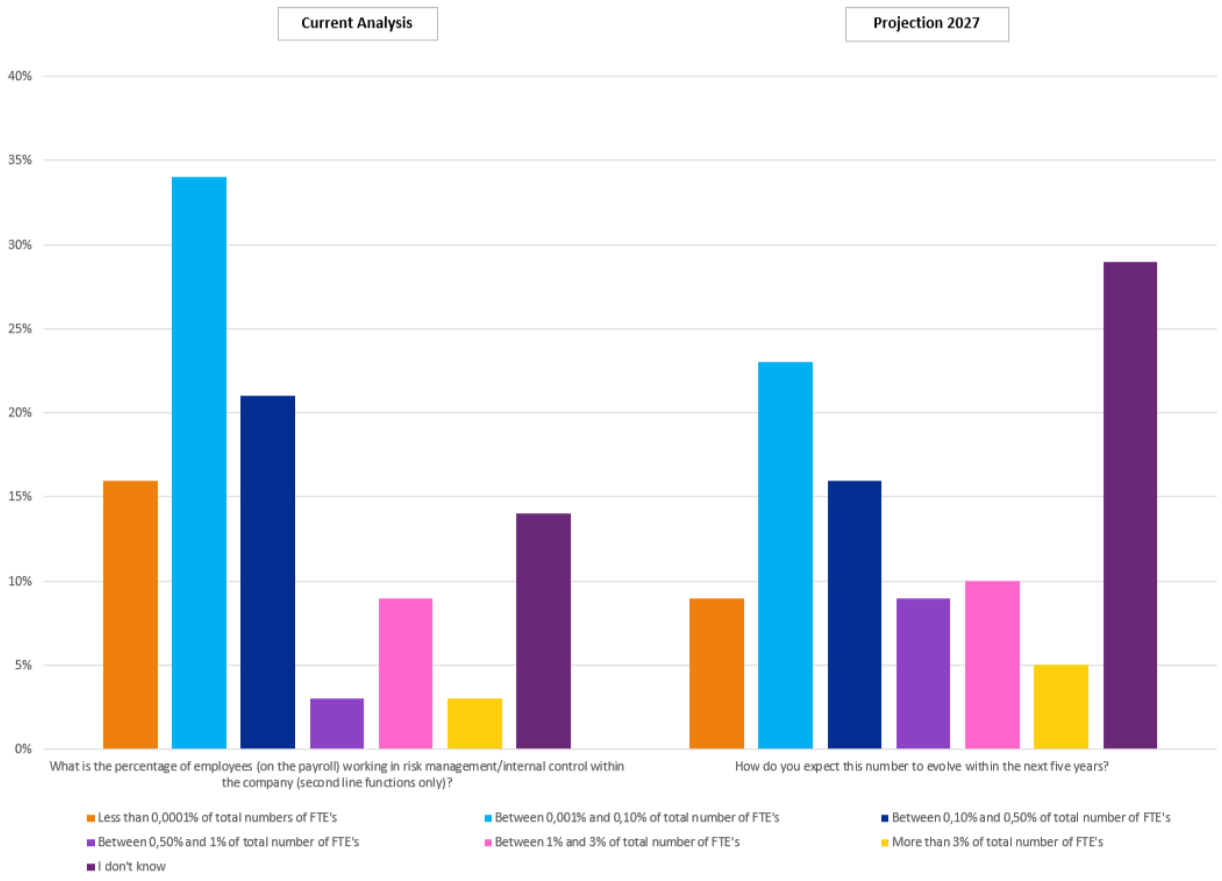
In this section the focus was to identify challenges faced by organisations to attract, retain and upskill their risk management workforce and the different strategies they adopted. As people and culture, both run through every aspect of a company, the survey assessed the extent risk was incorporated within the corporate culture.

Driving the employee retention strategy

35% of the companies stated that attracting talents with adequate experience and expertise was a challenge which could also be a direct consequence of recent trends such as the 'War for talent' and the 'Great Resignation' (Forbes, 2021). It was however highlighted by the Study that the expectations for the future demand of risk professionals was uncertain, as 28% of organisations forecast an increase in the numbers of FTE's in the future, while 44% believe it will remain the same and 29% do not know yet what their future workforce will look like. It is worth noting though that no companies showed any interest in decreasing its risk management workforce.

Identifying the profiles required to fill risk management positions is based on the strategy and financial resources and level of risk that the organisation is willing to take which should be governed by the top.

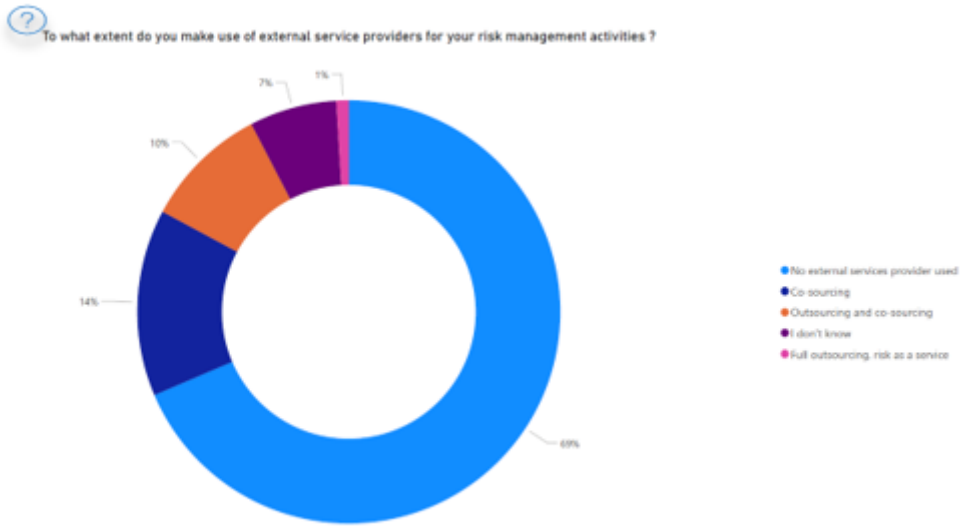
The absence of training and development plans in 50% of the companies indicates that organisations are struggling develop or implement talent retention strategies for risk management. Another reason for the absence of skills requirement and development plans could be the absence of a strong risk management structure as it was highlighted in prior segments.

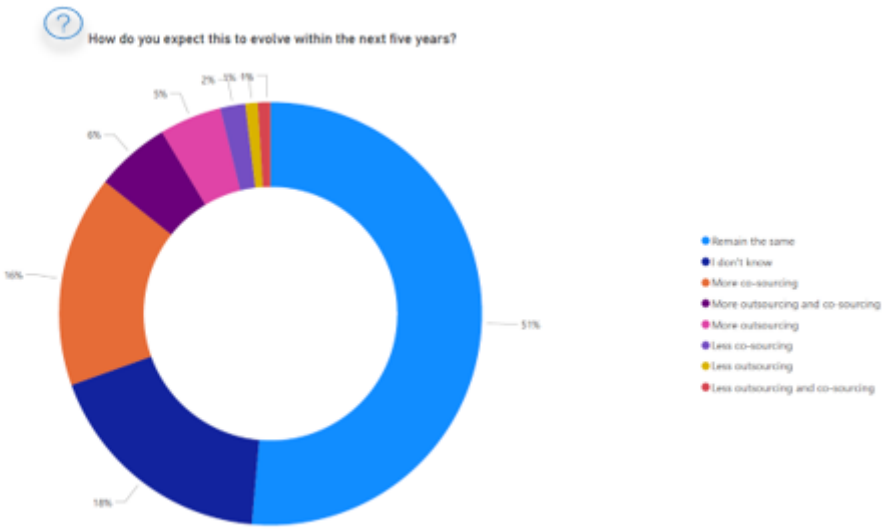


Given the strong demand for suitably skilled and experienced internal auditors, risk management experts believe that most organisations find it difficult to sustain their own risk and audit function. Talent retention is therefore important as the existing employees already master an understanding of the business environment and risks associated. Continuous training and development are also suggested to be key element to keep up with emerging trends.

Finding fitted services

Despite the in-depth knowledge and specific profiles required within risk management and the challenges to retain and attract risk management talent, 69% of the companies did not use external service providers for their risk management activities. Only 16% of companies, projects that outsourcing or co-sourcing will grow.



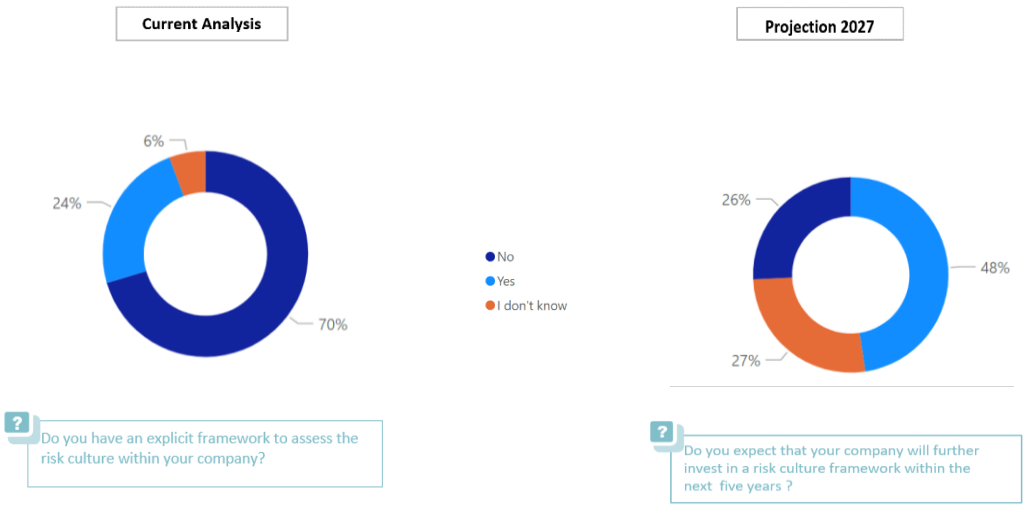


Emerging risks and specific risks can require specific skills which can be difficult and costly to maintain inhouse. This would explain the need for external providers who could bring their expertise to assist when required.

According to the interviewed risk management experts, a proper understanding of what the company needs in terms of expertise is essential to have an efficient risk treatment, therefore extending its risk management activity to an external provider when needed can prove to be beneficial to companies, while leaving the control of how processes are handled in the companies' hands. Moreover, this would allow companies to benefit from external experiences from the external providers, which they would not have received otherwise.

Understanding the risk culture

Building and embedding the desired risk culture and values is important to ensure a performing risk function. During the survey 70% of the companies admitted that they faced difficulties to understand and define their risk culture which is directly linked to the absence of a defined framework. 48% of these companies intends to work towards the implementation of risk culture. The risk culture should be aligned with the strategy and the risk appetite to have positive outcome on the company.



The IIA puts forth the soft control model to help companies assess their risk culture. The scope of this model is the culture but also how management and employees behave, linking those elements to the achievement of the company's objectives.

This type of control is an efficient tool companies which can represent a great opportunity for organisations using it. It can be used to support their employees' performance in terms of conviction and personality. As such, it can influence their "motivation, loyalty, integrity, inspiration, standards and values" (Institute of Internal Auditors, 2015). Employees' behaviours can be indirectly influenced by those elements.

To implement soft controls within a company, the IIA suggests companies to ask themselves questions related to the readiness of the company, whether or not they have the adequate structure to perform them. Moreover, companies should be clear about the results they expect. This implies having a clear definition of the risk strategy to know on which behaviour employees should align.

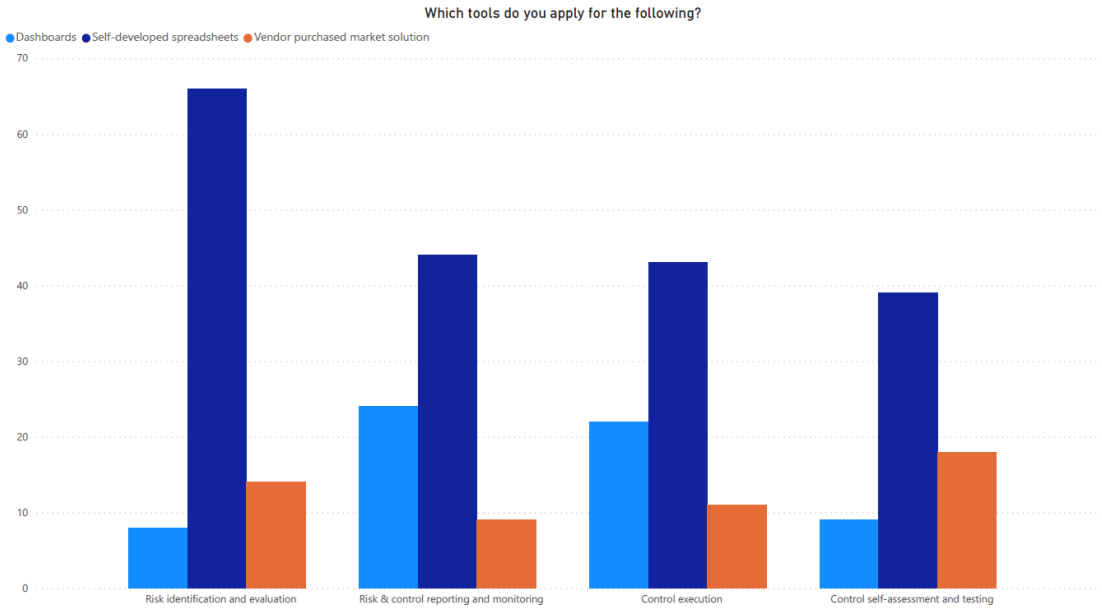
In terms of implementation, numerous approaches are possible, and companies should choose the one that suits it best. Those approaches include: exploratory research, directly testing the employees' results, making a cause analysis, doing an integrated audit, conduction a thematic audit or doing a behavioural audit (Institute of Internal Auditors, 2015)

3.2.7 Technology

The importance of technological solutions is increasing within all spheres of business activity. The possibilities it offers can change the way businesses are approached, including risk management topics through GRC tooling. Therefore, companies were reviewed to understand how far technology was incorporated within their processes, and the projected evolution over the next five years.

Building up assurance with the right tools

The survey pointed out that most companies did not have the adequate tooling for their risk management activities. 63% companies relied on self-developed spreadsheets, but these solutions, even though they can suit a company's needs to some extent, do not build assurance with respect to the information they support.

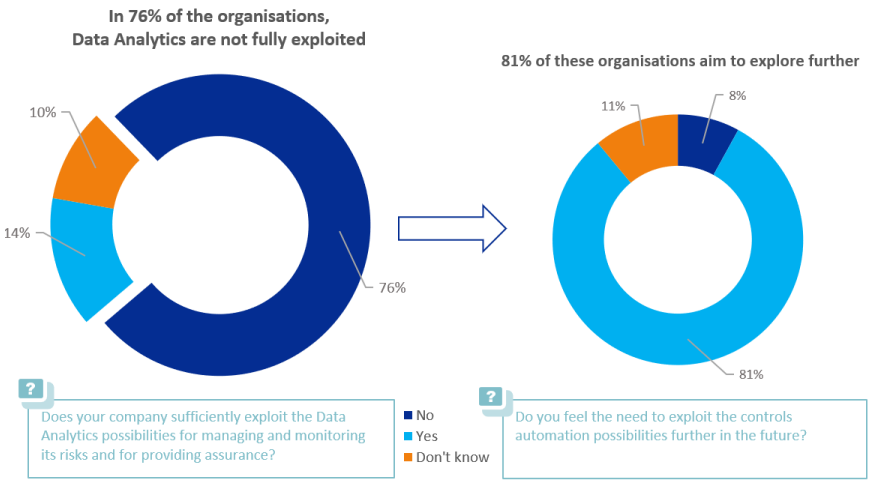


Building up assurance, is a challenge faced by most organisations. We learnt from the pandemic that growing towards a connected model has become a real necessity, as it enables clear communications between all the parties involved. The use of disconnected tools systems and processes accelerated inefficiencies within organisations and therefore, lowered the assurance levels.

Understanding the needs of the company will be the first step. Based on the capabilities available and the level of maturity of the company, further steps will be defined to enhance existing systems.

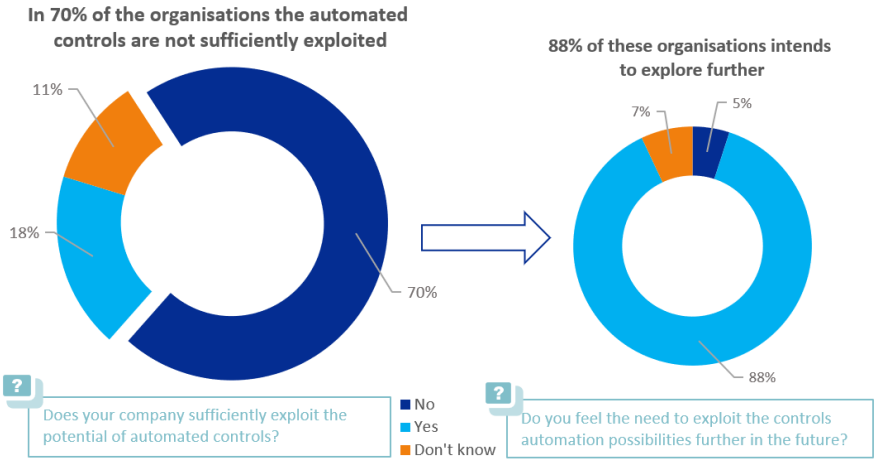
Exploiting all opportunities

The common consensus highlighted in the survey is that the majority of companies realise the importance to exploit the opportunities offered by Data Analytics and automation of controls.



A general tendency noted is that companies are moving towards a more proactive setup than before, a setup which will require a much more important flux of data than in the past.

According to the interviewed risk management experts, exploiting those data with connected tools will have a strong impact on the companies' activities and will require efforts to implement Data Analytics with the rest of the processes the company operates, so that the end message is both coherent and well understood across the whole company. It is therefore a major opportunity for companies to embrace.



Having advanced tools can be an advantage but the right profiles should be recruited to operate these them. A change management process should be triggered as some rooted habits may be complex to change. The benefits of moving towards the solution far outweighs the problems.

As explained by Hans Meulmeester (2022), an advanced GRC tooling will bring many benefits to companies. This can ease the process of compliance process with regulatory requirements. Moreover, using automated tools will not only reduce the human efforts and the risks of error that comes with it, but it will also give employees more time to focus on core activities. The level of expectations in terms of GRC practices will be significantly decreased and made more user-friendly by adopting automated alternatives. Implementing GRC tooling for risk management will also provide the different actors of the three lines model with clearer guidelines, such as automatic notification to the end user in case an action is required by the system, or automatic issue creation in case of failed attestations or controls. Linking all the element if the risk management system will create a more efficient and a more standardized way to approach risks and allow issues to be tackled in a timely manner.

It can also be highlighted that although automating the GRC tooling of a company implies a cost, it will also imply a decrease in the cost of the control, while having a standardized approach to manage the lifecycle of all controls and the regulatory changes that could affect risk management processes of a company.

4. Conclusion

To conclude this thesis, we will first explain once again the context in which this research was conducted and then summarize the main challenges and opportunities that were noted in order to try and shed the light on the challenges and opportunities for risk management in the non-financial sector.

Covid crisis, war in Ukraine, forecasts of a global recession; the risk landscape in which companies evolve has never been so uncertain. The risks faced by companies are unlike anything encountered in the past, the risks are more volatile, more interconnected, more dynamic, and increasingly digital in nature.

It is obvious that the evolution of the risk landscape requires a revolution of risk management practices. The situation is even more alarming in the non-financial sector as a lack of regulatory oversight could result in gaps in risk capability; failure to promptly respond to new situations; and lack of clarity for accountabilities, roles and responsibilities from the top leadership through to the day-to-day business.

In order to cope with the new reality we live in, risk transformation has become a necessity for companies so that they can become the success stories of tomorrow, risk transformation being the transformation of people and processes through the use of modern risk technologies.

The survey around risk transformation led for this thesis during our internship at KPMG highlighted the main areas that will reshape risk management practices over the next five years:

- Integration of governance and risk,
- Increased collaboration between the lines of defence,
- Shift towards a more dynamic risk management model; and
- The role of technology in the transformation

A striking element is how close those key findings are compared to the ones mentioned in the literature review presented in the first section of the thesis, as the points of integration of risk management, dynamic approach of risk management and the inclusion of more technology within the risk management processes are the highlights that struck out directly from the results.

Integration of governance and risk

Integration of governance and risk continues to be a complex challenge for organisations. The survey highlighted major improvements required to strengthen the governance structure.

One important feature was the absence of an integrated risk management framework governed by the Board in 30% of the organisations.

The lack of involvement of the Board in the design of the risk management framework can make it challenging considering the knowledge of risk and all the elements the Board must take into account in the decision-taking process.

Another factor linked to the finding was the lack of proper knowledge and skills at the committee's level. 50% of the survey respondents confirmed that upskilling of the Board committees would be the next focus area to strengthen the governance structure in the future. Not having a fully qualified or experienced committee undermines the effectiveness of the oversight role and can lead to difficulties to challenge arguments on risk management.

A crucial element for risk integration was a common understanding and approach regarding vision, strategy and roadmap which was missing in 52% of the organisations. The absence of a clear vision and strategy is one of the root causes for the absence of risk appetite framework and was noted in 62% of organisations. As a result, the same proportion of organisations were unable to measure the performance of an activity or of people. Another associated pain point was in terms of risk culture whereby most organisations admitted that they encounter difficulties to define their risk culture. This is because risk culture should be aligned to their strategy and risk appetites to ensure positive outcomes.

Most corporates surveyed intend to move towards a reinforced and integrated governance and risk management model in the future, offering these companies the opportunity to bring their risk management to a higher and more assured level.

More collaboration is expected between the lines of defence

Furthermore, it was noted that 65% of organisations perceived a shift towards more collaboration between the second and third lines of defence. This move will prevent duplication of efforts and ensure that a common message is delivered to senior management.

As per the survey results, most organisations assigned the risk ownership to the first line of defence and as per half of the respondents the risk strategy was not defined and applied. A common reason for risk strategies not being applied is the lack of coordination and alignment between the lines of defence. It is often observed that the strategy is not properly reflected in the actions taken by the first line of defence, due to a lack of understanding or a lack of communication with the second line of defence.

Increased collaboration between the lines of defence in the future will in turn present organisations with the opportunity to increase the importance, focus and effectiveness of risk management activities.

Shift towards a more dynamic risk management model

To succeed in this reinvention process and the turbulent times ahead, more dynamism and agility have become a necessity rather than an option for organisations. The adoption of this innovative and fresh mindset is still at an early stage based on the facts of the survey.

Analysis of the methods for risk identification revealed that most organisations were not prepared to anticipate and deal with rapid emerging risks as only 10% of businesses adapted their processes with new dimensions such as risk velocity and interconnectedness. The recent events in the world have shown that risks that were disregarded earlier because of their low likelihood, have to be considered from now on. Indeed, the same risks could be anticipated if velocity and interconnection with other risks were considered. Considering a very broad scope of risk has therefore become an opportunity for companies to embrace new tendencies as early as possible and not be caught in the storm.

Agility is the foundation of innovation and has been proven to support growth in organisations operating in highly dynamic environments. Only 10% of companies currently applies the agile methodology within risk management and only a quarter of the organisations that do not apply the methodology forecast to move in this direction in the future, even though this methodology offers a very proactive posture to its users.

Only a minority of organisations intend to rely on external providers for risk management, this will be a difficult and costly choice for the future as specific skills are required to deal with emerging risks.

We take the example of a business continuity and crisis management framework which was not implemented for 50% of the organisations which could be due to a lack of agility at corporate level to proactively identify and implement one or possibly due to a lack of expertise in-house. However, it is suggested that such frameworks are key opportunities for the viability of companies.

Risk management and technology

Risk management and technology are becoming more and more interlinked. As most businesses moved towards a connected way of operating and considering the growing need to process significant amount of data that is being produced daily, reviewing the use of technology within risk management was well timed.

The survey highlighted that the advancement in terms of technology was lagging behind for risk management as most companies surveyed still relied on manual tools to process their data. Only a minor percentage of these organisations embraced opportunities offered by IT solutions in risk management.

Another disclosure from the survey was the absence of embedded reporting and escalation protocols in 35% of surveyed business for which the root cause might be due to a lack of mechanisms or tools to measure and report risks and which could become a pressing matter given the growing quantity of data and the visualisation it requires.

Most businesses realised the importance of data analytics and controls automation. The amount of data that can be processed through the right tooling and efficiency gains is impressive and enables automatically enhanced processes which in provides a competitive advantage. Embracing fully integrated and automated solution is a long journey for many organisations, but with the promise of many opportunities for those who undertake it.

The practical approach of this thesis has emphasised the challenges faced by businesses not embracing the shift in technology within risk management and on the other hand exploiting what the changes could bring to the table for companies.

As mentioned in the introduction of this thesis, risk transformation is *"the continual evolution of an organization's risk function, systems and processes" (ISACA, 2019).* All the elements developed during the analysis of the results of the Study brought attention towards pain points companies were encountering in their risk management processes and how it could evolve for better within the companies' existing system, but the four elements pinpointed in this conclusion should most definitely serve as foundations for the years to come.

While many opportunities for companies have been developed in this thesis, it is important to mention that they should all be understood from a relative point of view based on the level of maturity of the company. Therefore, opportunities should be taken one step at a time and should take into account the organisation's maturity stage.

This research, by bringing into the light the current practices in risk management and the expectations companies had for the five years to come, has shown that the future of risk management lied in a dynamic and modern approach to this field. The recognition of risk management as a core activity of companies will without a doubt become a necessity for businesses to be viable and embracing the technology allowing the processing of all the data available will also represent a milestone in companies' development. Strong collaboration within the organisations will need to be present to support these first elements and ensure a coherent flow of information and actions. Those challenges, while being known, require due transformation within companies as it was presented in this thesis in order to turn them into opportunities and future years will either prove these findings right or show a totally different reality than the one many companies are currently preparing to, but one thing remains certain, risk transformation is happening in every company, one way or another.

5. Personal conclusion

Writing this thesis has proved to be more challenging than I expected, even though this is something we had been told about for the past 5 years.

Finding a topic worth researching was already a first challenge and I was fortunate enough to be introduced to the subject of risk transformation at my internship, which gave me a solid basis for my research.

However, I believe the process could have been pushed further given the data that was gathered. Indeed, the results regarding the types of respondents based on their location, revenues and number of FTE's were not investigated in this thesis. This was a voluntary choice as the amount of analysis and of descriptions deriving from those comparisons would have required a very long development which would not have fitted the thesis format. Aside from the practical aspect, it should also be mentioned again that the distribution of respondents was not balanced at all, so making those comparisons would not have provided us with the most relevant outcomes. Further studies however could pursue this possibility by balancing the sample and by trying to highlight patterns based on the identification factors applied to the companies.

Bringing the project further could also include an extension of the interviews discussing the survey results to a broader audience than only experts from KPMG such as actors of the three lines model, who remain the first concerned by this subject of reflection. Challenging the current insights could create more relevant conclusions, although I believe that the diversity of the interviews coming from the different KPMG member firms already brought a very thorough view on the outcomes. Still, all the statements made by the interviewed risk management experts should be treated with caution. Although it is not a commercial tool, it is obvious that the Study should be able to generate a need for services from readers and thus feed the consultancy services that participated in the redaction of the report. However, I believe that the way the interviews were approached (by addressing broad themes before revealing the results of the survey) allowed me to obtain a relevant view on the topics studied.

A last important limit I faced is my lack of expertise in the field of risk management. Although I intentionally started my thesis in an unknown field to challenge myself one last time during my studies, I quickly understood that bringing an expert paper to life with such a low knowledge of the topic at hand was not an easy task. I can't stress enough how important the help and reviews from the Risk and Assurance team was for this project, as they provided me with the proper understanding and the right phrasing, which I could never have achieved by myself.

References

7 KPIs You Can Use for Risk Management. (2021, September 10). Indeed Career Guide. Retrieved March 25, 2022, from https://www.indeed.com/career-advice/career-development/kpi-for-risk-management

20-July-2020 IIA Issues Important Update to Three Lines Model. (2020, July 20). Institute of Internal Auditors. Retrieved May 14, 2022, from https://www.theiia.org/en/content/communications/press-releases/2020/july/20-july-2020-iia-issues-important-update-to-three-lines-model/

Admin, W. (2020, December 17). *Fraud Risk*. Open Risk Manual. Retrieved March 14, 2022, from https://www.openriskmanual.org/wiki/Fraud_Risk

Alexander, A. G. (2021). Effective measurement of enterprise risk management programs. *Continuity Central*. https://www.continuitycentral.com/index.php/news/erm-news/6309-effective-measurement-of-enterprise-risk-management-programs

Awake Security. (2021, May 12). *Third Party Risk Definition & Examples*. Retrieved April 14, 2022, from https://awakesecurity.com/glossary/third-party-risk/

Bank for International Settlements. (n.d.). *MAR11 - Definitions and application of market risk*. BIS. Retrieved April 14, 2022, from https://www.bis.org/basel_framework/chapter/MAR/11.htm?tldate=20191216&inforce=20220101&published=20191215

Beaty, S. (2020, June 26). *Most interconnected risks (risk clusters)*. KPMG. Retrieved April 14, 2022, from https://home.kpmg/xx/en/home/insights/2020/06/most-interconnected-risks-clusters.html

BNY Mellon. (2021, April 12). *Risk Committee - Corporate Governance*. Retrieved March 17, 2021, from https://www.bnymellon.com/us/en/investor-relations/corporate-governance/risk-committee.html

Brasseur, K., & Brasseur, K. (2020, July 20). *IIA's 'Three Lines of Defense' updated to stress collaboration*. Compliance Week. Retrieved April 3, 2022, from https://www.complianceweek.com/risk-management/iias-three-lines-of-defense-updated-to-stress-collaboration/29212.article

Cau, D. (2013). *Governance, Risk and Compliance (GRC) software Business needs and market trends*. Deloitte.

Committee of Sponsored Organization. (2017). *Enterprise Risk Management Integrating with Strategy and Performance*. https://www.coso.org/Pages/default.aspx

Committee of Sponsored Organisations. (2017). *ERM Integrated framework*. COSO. https://www.coso.org/pages/erm-integratedframework.aspx

ComplianceOnline Dictionary- ERM Framework- COSO Components. (n.d.). Compliance Online. Retrieved May 12, 2022, from https://www.complianceonline.com/dictionary/COSO_ERM_framework.html

Corporate Governance Committee. (2020). *Belgian Code of Corporate Governance*. https://www.corporategovernancecommittee.be/en/over-de-code-2020/2020-belgian-code-corporate-governance

Council of Development European Bank. (n.d.). *Liquidity Risk*. CEB. Retrieved April 14, 2022, from https://coebank.org/en/investor-relations/risk-management/liquidity-risk/

Deloitte. (n.d.). *Cultural Risk and Your Organization's Reputation*. Deloitte United States. Retrieved April 14, 2022, from https://www2.deloitte.com/us/en/pages/risk/solutions/cultural-risk-reputation-management.html

DiPietro, B. (2015, April 29). *The Morning Risk Report: Companies Adopting Updated COSO Framework*. WSJ. Retrieved May 3, 2022, from https://www.wsj.com/articles/BL-252B-6902

Doe, C., & Gennarini, A. (2019, March 8). *Five objectives for the future of risk management*. EY. Retrieved April 28, 2022, from https://www.ey.com/en_be/financial-services/five-objectives-for-the-future-of-risk-management

Enterprise Risk Management Initiative Staff. (2004, September 1). *COSO's Enterprise Risk Management – Integrated Framework*. Poole College of Management. Retrieved May 12, 2022, from https://erm.ncsu.edu/library/article/coso-erm-framework

Eulerich, M. (2021). The New Three Lines Model for Structuring Corporate Governance – A Critical Discussion of Similarities and Differences. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3777392

European Banking Authority. (n.d.). *Operational risk*. Retrieved April 14, 2022, from https://www.eba.europa.eu/regulation-and-policy/operational-risk

Gjerdrum, D. (2016, February 22). *A Brief History of ISO 31000 – and Why It Matters*. Risk & Insurance. Retrieved May 3, 2022, from https://riskandinsurance.com/a-brief-history-of-iso-31000-and-why-it-matters/

Home | The Institute of Internal Auditors | The IIA. (2022). The Institute of Internal Auditors. Retrieved May 12, 2022, from https://www.theiia.org/

Howitt, J. (2021). Three Lines the Good, the Bad and the Ugly. *PRMIA : Professional Risk Managers' International Association*.

Institute of Internal Auditors. (2015). *Discussion paper Soft controls What are the starting points for the internal auditor?* IIA.

Institute of Internal Auditors. (2020). *THE IIA'S THREE LINES MODEL*.

International Organization for Standardization. (2018). *Risk management — Guidelines*.

ISACA. (n.d.). *Effective User Access Reviews | ISACA Journal*. Retrieved April 14, 2022, from https://www.isaca.org/resources/isaca-journal/issues/2019/volume-4/understanding-compliance-risk-in-finance-and-banking

ISO 31000 — Risk management. (2021, December 10). ISO. https://www.iso.org/iso-31000-risk-management.html

ISACA. (2019). *A Model and Best Practices for Risk Transformation*. Retrieved May 13, 2022, from https://www.isaca.org/resources/isaca-journal/issues/2019/volume-3/a-model-and-best-practices-for-risk-transformation

Jules, A. (2021a, August 30). *ISO 31000 Principles of Risk Management - ISO 31000 Training*. ISO 31000 Training - Premier Course. Retrieved March 15, 2022, from https://learn31000.com/iso-31000-principles-of-risk-management/

Jules, A. (2021b, August 30). *Risk Appetite vs. Risk Tolerance - ISO 31000 Training*. ISO 31000 Training - Premier Course. Retrieved May 12, 2022, from https://learn31000.com/risk-appetitive-vs-risk-tolerance/

Kelly, J. (2021, June 25). *The War For Talent And Great Resignation Puts Human Resources Professionals And Chief Remote Work Officers In High Demand*. Forbes. Retrieved May 14, 2022, from https://www.forbes.com/sites/jackkelly/2021/06/24/the-war-for-talent-and-great-resignation-puts-human-resource-professionals-and-chief-remote-work-officers-in-high-demand/?sh=5c21c1415fb9

Kohr, C., Thai, A., Johari, M., Aziz, S., Ong, J., Mahmood, M., & Kei, H. S. (2020). *Business Continuity Management Setup, updates and management*. KPMG.

KPMG. (2013). *Expectations of Risk Management Outpacing Capabilities – It's Time For Action*.

KPMG. (2021, May 17). *Nine thoughts about risk*. Retrieved May 5, 2022, from https://home.kpmg/be/en/home/insights/2021/05/blc-nine-thoughts-about-risk.html

KPMG. (2022, February 28). *Centralize risk and compliance with ServiceNow IRM*. https://home.kpmg/be/en/home/insights/2022/02/adv-centralize-risk-and-compliance-with-servicenow-irm.html

Dynamic Risk Assessment. (2019). KPMG. Retrieved May 5, 2022, from https://home.kpmg/au/en/home/services/audit/dynamic-risk-assessment.html

KPMG (2020, October 15). *Business continuity and resilience: key takeaways for boards*. KPMG. Retrieved March 15, 2022, from https://home.kpmg/be/en/home/insights/2020/10/blc-business-continuity-and-resilience.html

KPMG Target Operating Model. (2021, August 23). KPMG. Retrieved May 18, 2022, from https://home.kpmg/gr/en/home/insights/2021/08/kpmg-target-operating-model.html

Lam, J. (2014). *Enterprise Risk Management: From Incentives to Controls.* Wiley.

Lyons, S. (2020, July 22). *A critique of the IIA's Three Lines Model and its implications for Internal Audit*. LinkedIn. Retrieved April 15, 2022, from https://www.linkedin.com/pulse/critique-iias-three-lines-model-its-implications-internal-sean-lyons/

Margherita, A., & Heikkilä, M. (2021). Business continuity in the COVID-19 emergency: A framework of actions undertaken by world-leading companies. *Business Horizons*, *64*(5), 683–695. https://doi.org/10.1016/j.bushor.2021.02.020

Morgan, L. (2021, October 12). *Traditional vs. enterprise risk management: How do they differ?* SearchCIO. Retrieved May 12, 2022, from https://www.techtarget.com/searchcio/feature/Traditional-vs-enterprise-risk-management-How-do-they-differ

Parmenter, D. (2019). *Key Performance Indicators: Developing, Implementing, and Using Winning KPI´s*. Wiley.

Philbin, B., Bournival, V., & Petruska, K. (2013). *Risk Interconnectivity: Increasing Risk Intelligence at the Canada Revenue Agency*.

Principles behind the Agile Manifesto. (n.d.). Agile Manifesto. Retrieved May 3, 2022, from https://agilemanifesto.org/principles.html

Racz, N., Weippl, E., & Seufert, A. (2010). A Frame of Reference for Research of Integrated Governance, Risk and Compliance (GRC). *Communications and Multimedia Security*, 106–117. https://doi.org/10.1007/978-3-642-13241-4_11

Ripley, M. (2021). *Good Practice Guide: Risk Reporting*. Government Finance Function.

Risk management | Technical guidance | IIA. (2022, February 1). Institute of Internal Auditors. Retrieved March 14, 2022, from https://www.iia.org.uk/resources/risk-management/

The 2020 Belgian Code of Corporate Governance, Corporate Governance Committee, 2020

Societal Risk. (2014, December 18). AIChE. Retrieved May 12, 2022, from https://www.aiche.org/ccps/resources/glossary/process-safety-glossary/societal-risk

Star, E. (2021). *Risk Management 2025 and Beyond*. PwC. Retrieved April 28, 2022, from https://www.pwc.com.au/consulting/transforming-financial-services/risk-management-2025.html

What is a Key Performance Indicator (KPI)? (n.d.). KPI.Org. Retrieved March 20, 2022, from https://kpi.org/KPI-Basics

What is strategic risk? definition and meaning. (n.d.). BusinessDictionary.Com. Retrieved April 14, 2022, from https://web.archive.org/web/20181219045008/http://www.businessdictionary.com/definition/strategic-risk.html

Williams, C. (2020, September 7). *ISO 31000 vs. COSO – Comparing and Contrasting the World's Leading Risk Management Standards*. ERM Insights. Retrieved May 13, 2022, from https://www.erminsightsbycarol.com/iso-31000-vs-coso/

Yang, C. (2020, May 11). *Rethinking Agile: A Structured Approach To Risk Management*.

Forbes. Retrieved April 12, 2022, from https://www.forbes.com/sites/forbestechcouncil/2020/05/11/rethinking-agile-a-structured-approach-to-risk-management/?sh=1df00602cbe1

Young, P. (2021, April 29). *ESG risk management: building effective frameworks*. Grant Thornton UK LLP. Retrieved April 14, 2022, from https://www.grantthornton.co.uk/insights/esg-risk-management-building-effective-frameworks/