UNIVERSITY OF PIRAEUS
DEPARTMENT OF BUSINESS ADMINISTRATION
MASTER OF BUSINESS ADMINISTRATION
TOTAL QUALITY MANAGEMENT INTERNATIONAL (MBA TQM)

Master's Thesis

Diffusion of Enterprise Risk Management in Greek companies

Nikas Giorgos

Piraeus, 2020

ΠΑΡΑΡΤΗΜΑ Δ : ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ ΕΚΠΟΝΗΣΗΣ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΟΡΓΑΝΩΣΗΣ ΚΑΙ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

Μεταπτυχιακό Πρόγραμμα Σπουδών

στη «Διοίκηση Επιχειρήσεων – Ολική Ποιότητα» με διεθνή προσανατολισμό

ΒΕΒΑΙΩΣΗ ΕΚΠΟΝΗΣΗΣ Δ ΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

(περιλαμβάνεται ως ξεχωριστή (δεύτερη) σελίδα στο σώμα της διπλωματικής εργασίας)

Δηλώνω υπεύθυνα ότι η διπλωματική εργασία για τη λήψη του μεταπτυχιακού τίτλου σπουδών, του Πανεπιστημίου Πειραιώς, στη Διοίκηση Επιχειρήσεων - Ολική Ποιότητα με διεθνή προσανατολισμό με τίτλο:

Diffusion of Enterprise Risk Management in Greek companies

έχει συγγραφεί από εμένα αποκλειστικά και στο σύνολό της. Δεν έχει υποβληθεί ούτε έχει εγκριθεί στο πλαίσιο κάποιου άλλου μεταπτυχιακού προγράμματος ή προπτυχιακού τίτλου σπουδών, στην Ελλάδα ή στο εξωτερικό, ούτε είναι εργασία ή τμήμα εργασίας ακαδημαϊκού ή επαγγελματικού χαρακτήρα.

Δηλώνω επίσης υπεύθυνα ότι οι πηγές στις οποίες ανέτρεξα για την εκπόνηση της συγκεκριμένης εργασίας, αναφέρονται στο σύνολό τους, κάνοντας πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο.

Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου.

Υπογραφή Μεταπτυχιακού Φοιτητή/ τριας .....

Ονοματεπώνυμο Γιώργος Νίκας

Ημερομηνία 22/12/2020

To my parents, Michalis and Eleni…

Table of Contents

List of Tables and Figures

Tables

Figures

Acknowledgements

I would like to thank my supervising professor, Mister Markos Tsongas, for the valuable help he provided me throughout the thesis. I would also like to thank each and every one that took the time to participate in the survey and answer the questionnaire.

Abstract

In an extremely volatile business environment, all companies have to deal with a wide range of risks that pose threat to their organization longevity. Traditional risk management is not sufficient to handle modern risks or to fully take advantage of them. Risk management needs to be done centrally, across all the organization's functions, with a common approach and a common set of goals. Enterprise Risk Management can be used as a solution to this issue and if implemented properly can be used by any organization as a tool to help maximize its profits, minimize its losses, and increase the overall value generated.

One of the problems researchers face when investigating the implementation of ERM is the lack of a robust method for evaluating the level of implementation and integration of ERM in an organization's functions. This thesis addresses the aforementioned problem by proposing a reliable ERM measurement method. For the purposes of this thesis, a questionnaire was created which was communicated and answered by companies all over Greece. The data gathered were evaluated and graded with the use of dedicated grading matrixes which were then used as an input for a maturity model. Based on this information, the maturity level for each organization was assessed, as well as a general overview of the maturity level in Greece was defined. Furthermore, by analyzing the data, an insight was gained on the practices used by Greek companies regarding to risk management and the business tools that they use.

1. Introduction

1.1. Background and context

In a world overflowing with data and information it is very crucial for all organizations to be able to identify the threats and opportunities in their environment. Even though it is quite common in businesses such as investing or actuaries to focus on the potential scenarios that may arise from uncertain situations, the approach of most businesses use to be done in silo view, focusing on specific areas, and mostly dealing with the negative aspects and the repercussions for what could go wrong. As the years passed and with the changes made in the ISO 9001, ISO14001 and ISO 45001 standards, more and more organizations started to analyze the risks they were facing but, in most cases, there was no cross-function management of these risks.

Both risk and uncertainty can have major impacts on every organization, so it is apparent that they have to observe, manage and control numerous internal and external variables that affect the risk and uncertainty, as well as their potential outcomes. They are also concerned with their ability to predict and manage both positive and negative outcomes that result from various kinds of risk. The goal of every organization is to protect and create value for their shareholders by identifying and proactively managing risks and opportunities. Enterprise Risk Management (ERM) is the evolution of the traditional risk management and consists of the methods and processes used by organizations to manage their risks in order to mitigate their threats and take advantage their opportunities in the full scope of the organization. ERM offers a risk management system that typically involves defining specific events or situations related to the goals of the company, evaluating them in terms of probability and extent of effects, determining a response plan, and monitoring process.

Companies in Greece were on the verge of moving past the consequences of the financial crisis of 2009 when a new unforeseeable event occurred, the COVID-19 pandemic. In situations like this it becomes apparent that in order to manage the risk of an organization, sufficient preparation and appropriate infrastructure must be in place. This thesis will attempt to investigate the level of preparedness Greek companies have for dealing with uncertainty.

1.2. Research Objective and Questions

ERM can be a useful tool for any organization to achieve its objectives, in most cases by improving their performance. The recent global crises (both the past economic and the current healthcare) made proper risk management a necessity for all businesses. The importance of ERM and the growth of ERM implementation means there is a need for a reliable ERM diffusion measurement method to explore whether ERM practices can be found in organizations.

The findings of this research will provide empirical evidence of the diffusion of ERM in Greek companies, as well as identify which practices are being used in the country when it comes to risk management.

Within this thesis, the theoretical background of ERM will be presented, highlighting the core elements of an ERM system and the most prevalent frameworks. By the end of the thesis the following research questions will be answered:

- What is the level of diffusion of ERM in Greek Companies?
- What is the approach of Greek Companies regarding different risks?
- How familiar are Greek companies with different business tools related to ERM?

Lack of measurement and quantitative data is one the biggest problem when it comes to assessing ERM implementation. This thesis provides an approach to ERM measurement that can be applied to other segments of the global market and provide an overview of the ERM implementation. The scoring methods and scales used can also be implemented to other researchers when investigating the level of maturity if a process.

The finding of the research can be used as a basis for further analysis by other researchers, input materials by companies to improve their risk management performance or even, analysts and investors who require information about the current status of Greek companies.

1.3. Outline of the Thesis

This thesis will consist of six chapters. In the first chapter an overview of the study will be presented along with the aims and goals of the research. In chapter two the literature review will be conducted which will focus on providing the definitions for risk, risk management and enterprise risk management followed by an analysis of the basic

concepts of ERM as well as an overview of the most prevalent frameworks around ERM. In the next chapter the methodology of the research will be presented, including the creation of the questionnaire that was used for data gathering in this research. In chapter four the results of the questionnaire will be presented and in chapter five they will be further analyzed. The conclusion of the research will be presented in the last chapter. The questionnaire and the cover letter that was used for this research will be available in the annexes.

2. Literature review

2.1. Introduction

In this chapter the fundamentals of risk and risk management are established. Starting with a review of the terminology and the evolution of Enterprise Risk Management in the past years, an analysis of the relevant literature is done. Continuing, the focus is placed on the implementation of an Enterprise Risk Management system, its components, and the prevalent frameworks.

Risk is a part of everyday life and it affects both individuals and companies equally. No organization can avoid taking at least some risks, as this is a necessary part of its business activity and evolution. When facing a risk an organization must be able to identify it and assess its impact on the organization's goals. A risk can have outcomes that may be considered as positive, negative, or even both. This chapter explores the concepts of risk and uncertainty, as well as risk management, in the first section.

Continuing, the evolution of risk management is explained, based on the need for transition from the traditional approach. Enterprise risk management is seen as a solution to the problems of traditional risk management as, as it goes beyond the silo-based approach to of traditional risk management within an organization by taking a holistic approach. The purpose of this approach is to have a common method of risk management in an organization, that is oversighted by the management and is used as input in the decision-making process. As a result, internal, strategic, operational, compliance, reputational, and other complex risks can be dealt on a joint basis providing the ability to merge risk and achieve consistency.

In the final section of the chapter, the most prevalent enterprise risk management frameworks are presented with a deeper view on the ISO 3100 and the COSO frameworks. Even though the approach is different, similarities in the basic components of the two frameworks can easily be identified. This thesis will be based on these components, how can they be implemented in a company and how easily is it to identify them.

2.2. Enterprise Risk management

2.2.1. Risk Definition

Risk is a very common term, but it can have many connotations. According to (Lexico) the origin of the word risk comes "from the "French risque (noun), risquer (verb), from

Italian risco ‘danger’ and rischiare ‘run into danger’”. The Cambridge dictionary (1995) definition of risk is “The possibility of something bad happening”, whereas Oxford university’s (1884) is “a situation involving exposure to danger”. Both meanings emphasize the negative aspects of a risk and are used to show negative consequences. When the Society for Risk Analysis formed a committee to define "risk", concluded, that it might be better not to make such a definition. Kaplan (1997) said that each researcher should define and explain clearly what their risk definition is. It is therefore crucial in this thesis to set a basis of the definition of risk to have the right definition and link this "risk" definition with risk in the context of business.

The word risk, depending on the situation or who you may ask, can have many terms related to it such as danger, hazard, chance, probability, gamble, or uncertainty. Even though these terms are often used interchangeably, they can be very different. Risk can be attributed to the uncertain consequences that an event might have, which can be either positive or negative. There is a sense of the relative level of the event’s probability and is unlike uncertainty, which only considers an event where the probability is unknown (Pritchard, 2010).

Risk derives from uncertainty. According to Boritz risk is defined as *“the possibility of loss as a result of a combination of uncertainty and exposure flowing from investment decisions or commitments"* (1990). It can be said that risk is a mixture of uncertainty, possibility and chance that will happen in the future and can have both a positive and negative impact.

It is apparent that risk is everywhere, not only for companies, but also for anyone who experiences uncertainty about a future event that might result in an unexpected or adverse outcome. This can be called “risk”. Ansell and Wharton (1992) concluded that the meaning of the word “risk” has changed overtime *"from one of simply describing any unintended or unexpected outcome, good or bad, of a decision or course of action to one which related to undesirable outcome and the change of their occurrence"*. Therefore, risk can have a wide range from a positive to a negative event and it might be appropriate to apply the risk definition of Ansell and Wharton (1992) in this thesis, who said*: "A risk is any unintended outcome of a decision or course of action.".*

A description of risk has been given by several authors. Risk, in an organizational context is traditionally described as anything that can affect the achievement of the company’s goals, or as a negative event that could disturb performance. Hopkin (2012) summarized the definition of risk in the business context, as shown in Table 2.1:

Table 1 Definitions of risk (in the context of business)

Organization	**Definition of risk**
ISO Guide 73 ISO 31000 (2009)	Effect of uncertainty on objectives. Note that an effect may be positive, negative, or a deviation from the expected. Also, risk is often described by an event, a change in circumstances or a consequence.
IRM (Institute of Risk Management, 2002)	Risk is the combination of the probability of an event and its consequence. Consequences can range from positive to negative.
"Orange Book" from HM Treasury (HM Treasury, 2004)	Uncertainty of outcome, within a range of exposure, arising from a combination of the impact and the probability of potential events
Institute of Internal Auditors	The uncertainty of an event occurring that could have an impact on the achievement of the objectives. Risk is measured in terms of consequences and likelihood.
Alternative definition by Hopkin (2012)	Event with the ability to impact (inhibit, enhance, or cause doubt about) the mission, strategy, projects, routine operations, objectives, core processes, key dependencies and / or the delivery of stakeholder expectations.

Different definitions are presented to show that there is a wide range to the nature of risk that can have an impact in an organization. The International Organization for Standardization in its relative standard the ISO 31000, linked the risk with the effect it may have in the organization's objectives. The same approach is taken by the Institute of Internal Auditors. The UK government and the IRM take a more general approach focusing on the probability and consequence of events, which may be more easily applied. The term risk is defined in very different ways by many organizations, institutes, and scholars, additionally over the years new terms have been discussed the complicate the meaning even further. To that point, Hopkin proposed his definition for business risk to be *"An event with the ability to impact (inhibit, enhance, or cause doubt about) the mission, strategy, project, routine operation, objective, core process, key dependencies and/or the delivery of stakeholder expectations"* (Hopkin, 2012). The aim of this definition is to bring the word risk into organizations in a practical way.

To sum up, enterprise risk involves any risk or uncertainty that consist of both negative and positive outcomes. When facing the downsides, the goal is to minimize the surprise factor as well as any kind of loss by applying detection, preventive, and provision measures. On the other hand, for the positive outcomes, the goal is to be able to take advantage of the opportunity and maximize the gain an organization can get from it.

2.2.2. Risk management evolution

Risk management has evolved over time from a basic risk transferring approach, to structured systems forming an integral part of core enterprise functions, driven by compliance risk management regulations. When a risk arises, the way anyone chooses to interact with it can be considered as management. From the appearance of the homo sapiens and his decisions on how to handle the many uncertainties of his environment, to the highly regulated field of Finance and Banking the management strategies vary by a wide margin.

In business context, it is clear that insurance may be regarded as the first stage in risk management. Even as far as the 17th and 18th century, when ships sailed to the new world, before departure there were deals and contracts in place that could compensate both ship owners and crew members in case of specific things going wrong. An organization can control risk by reducing possible negative consequences through insurance.

Formal risk management programmes traced back to the 1950s as a result of the insurance management function in the US, and the emergence of the concept of contingency planning emerged in the 1960s, which became essential to businesses. The high costs of insurance and as it was insufficient to fully cover businesses, risk management became a more prevalent method to safeguard assets and control the business operation. At this point, risk management would initially concentrate again on managing only the downsides, with no consideration of the possible upside of events (Buehler, Freeman, & Hulme, 2008). During the 1970s emphasis was placed on the concept of cost-benefit and effective risk management transitioned along this path leading the total cost of risk consideration in the 1980s. Financial institutions and the adoption of project management techniques, helped the integration of risk and financial prospective and in 1990 we start to see the use of risk management tools and practises in order to deal with market, credit and operational risk for financial institutions. The next step in the evolution process the need to protect shareholder value so there was a

transition from insurance to the concept of protecting the business. Risk management evolved into accepting and taking advantage of the fact that risk may have both positive and negative outcomes and that insurance actually is just one way of dealing with potential hazards and risks.

In the early 1990s the term “Traditional Risk Management” (TRM) (Power, 2004)comes in play a risk involves the external environment of the organisation including aspects like: competitors, legal, medical, markets; business strategies and policies: capital allocation, product portfolio, policies, business process execution: planning, technology, resources; people: leadership, skills, accountability, fraud; analysis and reporting: performance, budgeting, accounting, disclosure and technology and data (Stroh, 2005).

At the eve of the 21st century the paradigm shifted from the transfer of the risk to third parties, to the optimal management of the risk and opportunities by minimising the level of risk itself (Hopkin, 2012). Even though opportunities and hazards were considered equally, the effective risk management was hindered by the fact that risks were regarded on a “silo” basis, meaning each process would manage the risk affecting their operations individually in a way that fitted their structure and their capabilities.

Major financial scandals including Enron, Worldcom, Bernand Madoff, etc. showed that organisations should adopt an overarching risk management system, something that was highlighted by the Sarbanes-Oxley Act of 2002 in the US. The role of Chief Risk Officer was created and the transition to Enterprise Risk Management (ERM) was considered in corporate governance as a solution to the problems of the Traditional Risk Management. Many ERM frameworks where formed at this time, as the financial crisis of 2008 showcased the need for a more holistic approach than the TRM and the necessity of an approach that would handle both external and internal risks, with the goal of increasing the shareholder’s value.

Similar to the definition of risk, the definition of risk management varies and depends on who provides them as shown in Table 2.2 (Hopkin, 2012).

Table 2 Definition of risk management

Organization	**Definition of risk**
ISO Guide 73 *ISO 31000 (2009)*	Coordinated activities to direct and control an organization with regard to risk
IRM (Institute of Risk Management, 2002)	Process which aims to help organizations understand, evaluate and take action on all their risks with a view to increasing the probability of success and reducing the likelihood of failure
"Orange Book" from HM Treasury (HM Treasury, 2004)	All the processes involved in identifying, assessing and judging risks, assigning ownership, taking actions to mitigate or anticipate them, and monitoring and reviewing progress
London School of Economics	Selection of those risks a business should take and those which should be avoided or mitigated, followed by action to avoid or reduce risk
Business Continuity Institute	Culture, processes and structures that are put in place to effectively manage potential opportunities and adverse effects

Hopkin (2012) concluded that the proper definition may be *"The set of activities within an organisation that is undertaken to deliver the most favourable outcome and reduce the volatility or variability of that outcome."*.

Throughout time the goal of risk management has been the same, to control uncertainty to the biggest degree possible and ensure the best possible outcome for the goals of the organisation.

2.2.3. Enterprise risk management

Enterprise risk management differs from the traditional version in the way it approaches each risk. ERM bring the integration and holistic view that is missing from TRM by combining different types of risk and integrating them into the organisation's overall

objectives (Rodriguez and Edwards, 2009). In contrast, TRM often is a victim of tunnel vision by using a silo-based approach. Silos are formed when an organisation handle each type of risk as separate inputs and with no consideration or evaluation on the implications to other risks and aspects of the organisation (Pagach & Warr, 2010). ERM promotes a better platform that allows organisations to have a better image of all the foreseen risks and thus, gives them the opportunity to effectively evaluate, prioritise and determine which risks should be accepted, mitigated or avoided in an holistic review process. With the use of ERM, the appropriate risk management strategy is formed by adopting an enterprise-wide risk management process with the participation of employees from all levels and positions in the organisation (Rodriguez & Edwards, 2009). According to Banham (2007) the essential differences between TRM and ERM, are shown in Table 2.3.

Table 3 Essential differences between TRM and ERM

TRM	ERM
Risk as individual hazards	Risk in the context of business strategy
Risk identification and assessment	Risk portfolio development
Focus on discrete risks	Focus on critical risks
Risk mitigation	Risk optimization
Risk limits	Risk strategy
Risks with no owners	Defined risk responsibilities
Haphazard risk quantification	Monitoring and measuring of risks
"Risk is not my responsibility"	"Risk is everyone's responsibility"

2.3. Strategic and Business Risks

A risk is can be categorised as "strategic" (may it be an opportunity or a threat) if it has the capability to affect an organisations viability. In their 2006 published paper, Neil Allan and Louise Beer (2006) explored how organisations and different management systems acquire information from both the external and internal environment in order to properly handle these types of risks. The study showed that most risk management systems had a weakness in the evaluation of strategic risk due to the dependency on qualitative approaches in the lines of statistical analyses and historic data that could not provide sufficient future forecasts.

There are many techniques that an organisation can use in order to identify its risks (strategic or otherwise). For example, staring with a PEST analysis (Political, Economic, Socio-Cultural & Technological macro-environmental factors) leading to the SWOT analysis (identification of Strengths, Weaknesses, Opportunities & Treats) is one of the simplest ways to classify risks coming both the organisation internal and external environment. Porter's Five Forces Analysis could be considered an advancement to SWOT analysis, even though Porter's method focuses on the competition in the market. By assessing the threat of substitutes, the threat of new entrants, bargaining power of suppliers, bargaining power of buyers, and industry rivalry the competitiveness of an industry can be determined so the organisation can set its strategic objectives based on the competition and the specificities and current status of the industry. This could be seen as a risk assessment done prior to deciding the strategic objectives in the organization

In order to achieve an effective management of strategic risk an organisation should follow five critical steps (Frigo & Anderson, 2011):

1. Assess the maturity of the ERM practices related to its strategic risks
2. Conduct a strategic risk assessment
3. Review the process for strategy setting, including the identification of related risks
4. Review the processes to measure and monitor the organization's performance (Key Performance Indicators)
5. Develop an ongoing process to periodically update the assessment of strategic risks

From another point of view, Levine (2013) suggested the Goals-Progress-Strategy (GPS) method for the management of risks related to strategic objectives. The 3 phases of this method consist of the clear articulation of the strategic objectives (Goals), followed by the establishment and monitoring of indicators and progress measures (Progress), and finally based on the results of the other two phases the refinement of the Strategic elements such as "*business tactics, risk mitigations, go/no-go decisions or overall strategic course*" (Strategy).

It is evident that the silo approach of the TRM does not suffice to manage the biggest and most crucial risks of an organisation, and in order for an ERM to be able to do, it must be grow into a high level of maturity. ERM serves as a tool used to minimise viability hazards and enables organisations to gain significant advantages when it comes to opportunities. Once the organisation reaches the necessary level of maturity and adopts

the appropriate risk management practices, it will greatly be benefited by acquiring a risk-based outlook and therefore a risk-based knowledge.

2.4. Basic components of an Enterprise Risk Management system

This section summarises the basic concepts of an effective Enterprise Risk Management system. Separated in 4 distinct phases, the core elements that should be evident in every ERM system are presented. Even though depending on the organization and its context, they may differ in the approach and possibly in the terminology used, these phases can be used to identify the process of ERM in every organization.

2.4.1. Understanding of the context and implementation of basic structures

Risk governance consists of all processes and mechanisms used for making decisions about which risks are taken and how they are implemented (Renn, 2008). In order to achieve the optimal results, an organisation must facilitate the needs of the selected risk management system by establishing internal structures such as processes, policies, reporting and recording tools etc. These structures must be integrated to the existing management system and the goal is to cultivate a common risk management culture, understood and followed by everyone int the company.

A lot of risks may be connected to different aspects of the organization, and when different risk owners within the organization individually manage risks separately (silo approach) the organization may lose significantly in value creation, if it does not address them in conjunction with each other. Starting from basic concepts like having a common risk language, to the creation of a common risk registry, the organisation must transition from the TRM method of silos to the το adoption of a common approach when it comes to risks. The basic concept of ERM is to pivot from the separate management of risks, to a unifying and more integrated approach to managing overall risk (Hoyt & Liebenberg, 2011).

Depending on each organization, different methods may be the correct choice. Enabling effective risk assessment and appropriate risk treatment requires a thorough understanding of the of the context of the organization and establishment of the scope the ERM is applied.

The first requirement of ISO 9001 is the understanding of the organisation and its context. According to the standard*: "The organization shall determine external and internal issues that are relevant to its purpose and its strategic direction and that affect its ability to achieve the intended result(s) of its quality management system. The organization shall monitor and review information about these external and internal issues."* (Quality management systems — Requirements). This is a generic approach that should be followed when it comes to the applications of ERM as well. The fist step in the design and implementation of the ERM is the understanding of the need and expectations of the interested parties, the mapping of the processes of the organisation, and the scope that the ERM is applied. Since all the above can change with time, the results of this process must be reviewed and revised often.

At this point, apart from the internal environment the organization must also assess the external environment which should include the social and cultural, political, legal, regulatory, financial, technological, economic, natural, and competitive aspects. Depending on the situation the scope of the analysis may be international, national, regional or local to define the key drivers and trends that could affect the objectives of the organization.

Before an organization can begin to effectively manage its risks, a clear set of objectives must exist, including a vision and operating principles. Upon establishment of these concepts, they must be clearly articulated and communicated to every member of the organization (depending on the impact they have on them). Unless there is a clear strategy and clear goals, risk management cannot be efficient since with no vision of the "end goal" there is no way to assess what is the best way to reach it. The objectives must also be quantified so the results can be evaluated accordingly.

When these objectives are set, the company must have a clear philosophy towards risk management. The organization's risk appetite, the context of the organization, its values, and its code of ethics will dictate what this philosophy is. ERM safeguards that there is a process in place to align the objectives with the established risk philosophy and risk appetite. The term "Risk Appetite" relates to the amount and type of risk that an organization is willing to pursue or retain (International Organization for Standardization, 2009) and should not be confused with the term "Risk Tolerance" that describes the acceptable level of variation relative to achievement of a specific objective (Rittenberg & Martens, 2012). The Management of the organisation sets the objectives and then (with the concurrence of the appropriate stakeholders) articulates the risk appetite that is to be applied for the pursuit of this objective. The extend that the organisations considers

the objective achieved or not achieved is defined by the risk tolerance. Both concepts are crucial to the ERM as guideline for the diffusion of the risk culture and as benchmarks of the outcomes of the process.

2.4.2. Risk identification

The first step in risk management is the risk identification. An organisation must be able to perceive changes in its environment and deduct any risks occurring from them. In order to do so, the organisation must have the appropriate receptors in place for all aspects of its operation. These receptors vary allot, depending on the complexity of the environment and the stakeholders related to the organisation, and must work in conjunction with each other. One of the simplest methods of risk identification is the consultation of members within the organisation as they can have a better view on many issues that the management at another level my not be able to perceive. There is no singular risk identification method that is able to cover everything, so should be several of should be in place at any given time.

Having identified the risks, next comes the assessment. There are many techniques for risks assessment, such as the Bayesian analysis, Business impact analysis, Cause-consequence analysis, Fault tree analysis, Monte Carlo simulation, etc. so depending on the risk at hand the appropriate method should be used. in order to identify the gravity of a risk, the simples (and most common) way is to define the likelihood of the risk happening and the consequences it may have on the objectives of the company it this happens. Risk matrixes are widely used to depict this approach, where the values of the aforementioned variables are multiplied, and a total is calculated. In an Enterprise Risk Management system, the final assessment of any risk must be comparable to any other risk assessment, and the terms and scales used compatible with each other. This is one fundamental aspect of ERM, the transition from a silo approach where each function deals with its own risks, to a unifying approach where all risks are evaluated in conjunction with each other.

Based on the assessment of the risks and the risk appetite, a prioritisation of the risks take place. It is not realistic to assume that all identified risks will be address at the same time, so a prioritization ranking must take place. The final ranking order can be the result of different factors such as the gravity of the risk, the available resources at the time of the assessment or in the future, or the impact on the organisation’s objectives.

All risk identified an any point, regardless of the outcome, should be recorded in an accessible risk registry. In this registry both horizontal (affecting one function) and vertical (affecting several functions) risks should be found and used to facilitate future risk identification and assessments.

2.4.3. Risk treatment

When a risk has been identified and properly assessed, the next step of the enterprise risk management process is to plan and perform the necessary actions to control it. From here, an organisation can choose to avoid, accept, share, or reduce any risk. One of these courses of action is followed for each event based on a company's risk appetite and tolerance. During the planning of the actions, it is important to include control points for each risk, so efficient monitoring can be achieved. All actions decided must also include the planning for the required resources, including time and manpower.

Every selected risk must have an appointed risk owner. In a silo approach risk owner might ignore significant risks that they consider to be outside their own operation or business unit. Therefore, it is crucial for an organization to have risk awareness, be accountable and take more proactive action to manage risk in a holistic way that will increase the value created (Barton, Shenkir, & Walker, 2002). Enterprise Risk Management requires all employers that manage risk outside the scope of their own work to take more responsibility and improve coordination than they do with traditional risk management.

2.4.4. Communication and monitoring

The last component of an ERM system is the way it tracks its performance and communicates its results. The purpose of monitoring is to ensure that the overall risk management process is executed and controlled as the planning process is constructed and actively proceeds. Monitoring is an essential component needed to achieve effective risk management, which must be done on a timely basis and integrated into every process as a part of the general culture (Chapman, 2012). It can be used to compare the outcomes of the process with the results predicted by the risk assessment and therefore improve future performance. Also, data coming from the monitoring can be used as inputs for the process in a feedback loop, for example identifying new threats and

opportunities, or help in the better understanding of upcoming risks. When possible the outcomes of the ERM should be verified and validated. Verification involves checking that the analysis was done correctly. Validation involves checking that the right analysis was done to achieve the required objectives (ISO Guide 73, Risk Management - Vocabulary).

Communication is crucial to the implementation of all risk management procedures and the monitoring of risk in general. Any information regarding risk must be communicated in an appropriate manner and in good time. Appropriate communication methods must be active across the organization, at every level. Furthermore, a common set of reports need to be established across the organization to assure common terminology and avoid time wasted interpreting unfamiliar formats. Common reports ensure the all risks are communicated and understood every stakeholder and provide timely information on the current risk position and trends, initially top-down, then drilling down to the root cause.

The purpose of all the above actions is to include the outcomes of the risk management process into the decision-making process from the management. Even if the process is applied correctly and all aspects are integrated in the day-to-day business of the organization, unless the information created is not used where necessary minimal value will be created.

2.5. ERM frameworks

In this section the most prominent ERM frameworks and risk management standards are examined, presenting their similarities and differences. The need of structured risk management practices in organisations that could have high applicability in different fields of business and regions led to the development of numerous risk management frameworks and standards by academics, practitioners, and guidance-setting organisations from different backgrounds (financial, insurance, safety, government, environment, engineering fields etc.), or international standard bodies. The aim of these frameworks is to provide guidance on the effective risk management approach, while providing a thorough analysis on the basic principles and the implementation methods.

Various risk management frameworks and standards are available worldwide, including self-assessment models, generic, problem or industry-based frameworks and standards, which provide standardised guides and measures recommended for developing successful risk management programmes. Based on a worldwide survey conducted by

the International Organization for Standardization (2011) the two most prevalent risk management standards were ISO 31000 (Risk Management Guidelines) and the COSO 2004 ERM frameworks (with the newest version arriving in 2017), so the thesis will focus mostly on them. The chosen framework and standard will be examined from a general and comparative perspective of their practical aspects.

2.5.1. ISO 31000 Standard – Risk Management Guidelines

ISO 31000 was published in 2009 (ISO31000, 2009) as the Principles and Guidelines on Implementation by the International Organization for Standardization, which was revised from the Australia/New Zealand risk management standard (AS/NZS 4360). The current version (at the time of writing) was published in 2018 and it describes a set of guidelines intended to streamline risk management for organizations. According to the standard *"[ISO 31000 is designed to be used by] any public, private, or community enterprise, association, group or individual."* (International Organization for Standardization, 2018) .

The risk management standards of ISO 31000 intent to be used widely, across all industries, organisation, and business types, to offer the best structure and guidance to all operations regarding risk management. Same as other ISO standards, ISO 31000:2018 is part of a larger family of risk management standards, generally referred to as ISO 31000. The current version of ISO 31000 family consists of:

- ISO 31000:2018 (Risk management — Guidelines)
- EN IEC 31010:2019 (Risk management — Risk Assessment Techniques)
- ISO Guide 73:2009 (Risk Management — Vocabulary)

These standards work in conjunction with each other as provide the tools for the understanding, evaluating, and managing risks in a way that can be applied to all organizations regardless of their size or composition. ISO 21500 (Guidance on project management) could also be considered as a part of this family as it includes integrating project management principles with ISO 31000 for risk management.

ISO 31000:2018 is also designed to connect with the High-Level Structure (HLS) introduced in the latest revision of ISO 14001 standard (Environmental Management) and adopted by the other commonly applied standards ISO 9001 (Quality Management) and the recent ISO 45001 (Occupational health and safety).

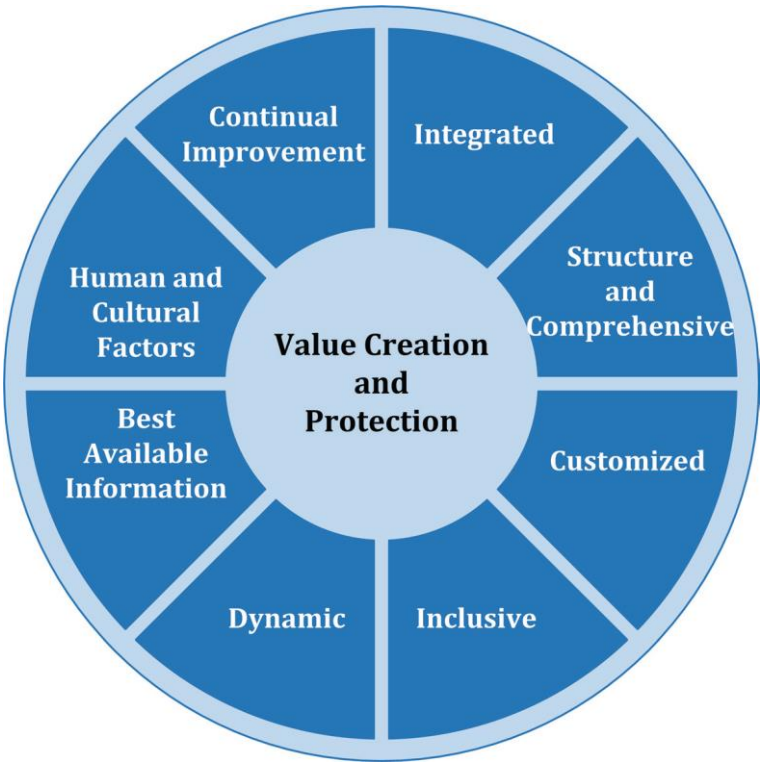
Table 4 HLS and ISO 31000 structures

HLS structure	ISO 31000 Structure
1. Scope	1. Scope
2. Normative references	2. Normative references
3. Terms and definitions	3. Terms and definitions
4. Context of the organisation	4. Principles
5. Leadership	5. Framework 5.1. General 5.2. Leadership and commitment 5.3. Integration 5.4. Design 5.5. Implementation 5.6. Evaluation 5.7. Improvement
6. Planning	6. Process 6.1. General 6.2. Communication and consultation 6.3. Scope context and criteria 6.4. Risk assessment 6.5. Risk treatment 6.6. Monitor and review 6.7. Recording and monitoring
7. Support	
8. Operation	
9. Performance evaluation	
10. Improvement	

With the focus on the risks and opportunities in ISO 9001, 14001 and 45001 standards the use of (HLS) helps to avoid confusion, misunderstandings and produces less duplication. Even though ISO 31000 is not certifiable, auditors (internal or external) and practitioners will have the ability to use a core set of generic requirements across different industry sectors. The International Organization for Standardization intents to transition to the HLS structure in all management system related standards, as well as use common terms and definitions.

As seen in figure 2.5 the standard consists of 8 core principles whose purpose is to create value for the organisation.

Figure 1 ISO 31000 Principles



(International Organization for Standardization, 2018)

These principles clearly describe the most important factors for an effective and efficient risk management framework, according to ISO 31000.

Following the standard presents the framework itself with the definition being *"a set of components that support and sustain risk management throughout an organization"* (International Organization for Standardization, 2018). Specifically, ISO 31000 defines six distinct areas that make up the framework for risk management with the most crucial being "leadership and commitment" so it is placed in the middle in figure 2.6.

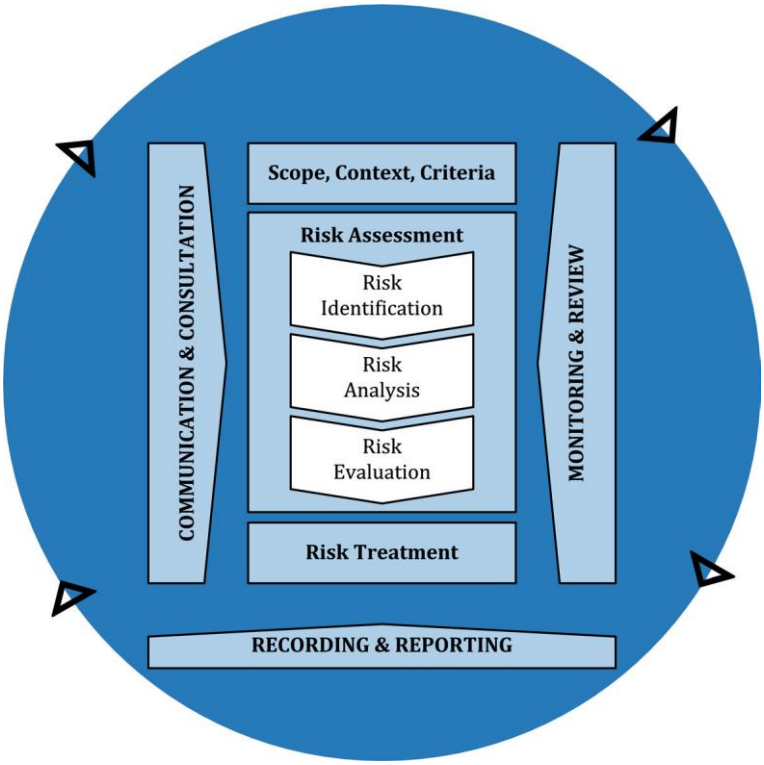
Figure 2 ISO 31000 Framework

(International Organization for Standardization, 2018)

The eight principles presented above are connected to the areas defined in the standard's framework. The principles act like objectives, describing what needs to be done, and the framework provides the necessary information on how to achieve those objectives.

The final part of the standard describes the management process which involves the use of policies, procedures, and practices to the activities of communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording, and reporting risk. The core building blocks is the risk assessment and treatment with the fist containing all actions needed in order to get the best possible input, and the latter focuses on the response to each risk depending on the organisations risk tolerance and appetite. This process is illustrated in Figure 2.7

Figure 3 ISO 31000 Process



(International Organization for Standardization, 2018)

2.5.2. COSO Enterprise Risk Management – Integrated Framework

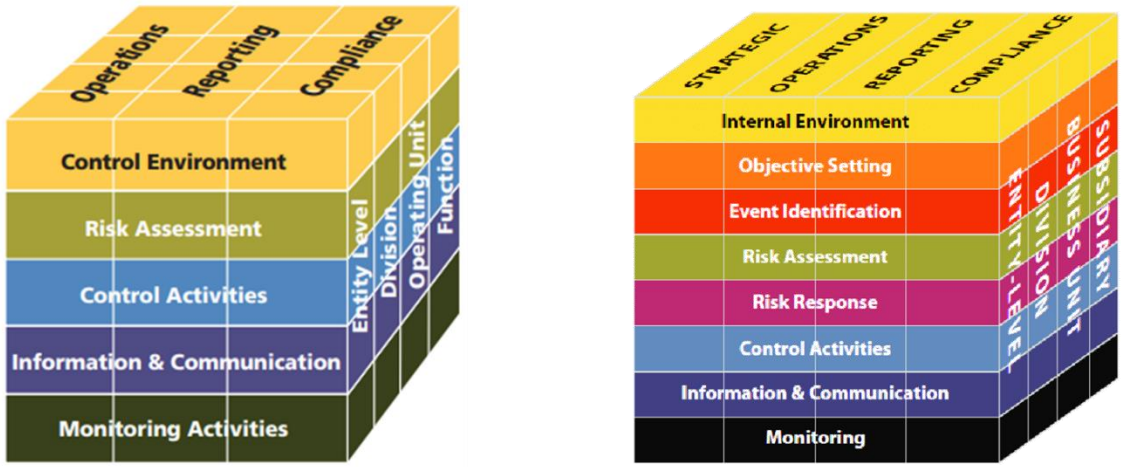
The Committee of Sponsoring Organizations of the Treadway Commission (COSO) was organized in 1985 to sponsor the National Commission on Fraudulent Financial Reporting, an independent private-sector initiative that studied the causal factors that can lead to fraudulent financial reporting. It also developed recommendations for public companies and their independent auditors, for the SEC and other regulators, and for educational institutions.

The first ERM related publication by COSO in 1992 was the (Internal Control – Integrated Framework). It provided a comprehensive framework for organizations to assess and improve their internal control systems and was very popular, especially in the USA. In the following years, as a result of the big financial scandals like Enron and regulations like Sarbanes-Oxley Act, organizations started to realize there was a gap in the internal control framework. While it was effective in minimizing risks related to fraudulent behaviour and regulatory compliance, it was unable to assess which risks the organization needed to control. This realisation led COSO in cooperation with the public

accounting firm Price Waterhouse Cooper (PWC) to create a new framework in 2004, the (Enterprise Risk Management – Integrated Framework).

Both frameworks use a three-dimensional cube to depict their core content. The face of the cube presents the risk management process components, the top slices the entity's objectives, and the side columns are the organizational units of the entity.

Figure 4 COSO 1992 and 2004 cubes



(COSO, 1992) *&* (COSO, 2004)

As seen in figure 4, the transition from just an internal control framework to a full scale ERM approach was done with the addition of some core elements. “Strategic” was included as a new objective, related to the strategic goals of the organisation. Furthermore, the existing five management components (Control Environment, Risk Assessment, Control Activities, Information & Communication, Monitoring Activities) expanded with tree new ones, the Internal Environment, the Event Identification, and the Risk Response to reach a total of eight.

Although, the 2004 version included strategic objectives as a category, the reason for including it was to ensure the organization’s strategies “align with operations, reporting, and compliance activities.” (COSO, 2004). This framework focused more on what can be audited rather than managing threats and opportunities, which provides the actual value of ERM, with many practitioners feeling that the solely concern was internal control.

In June of 2017, COSO published a new ERM framework titled (Enterprise Risk Management Framework - Integrating Strategy and Performance). Even though it did not introduce many new concepts, its focus on the integration of ERM with strategy-setting and performance with a deeper consideration on the role of corporate governance

and culture. Even with a glance at the new proposed structure it was apparent that there was a shift from the traditional and rigid cube to a new flowing double helix.

Figure 5 Components of ERM - 2017 COSO Standard

(COSO, 2017)

The new framework is now depicted with five components in different colours positioned between intersections of the multi-coloured ribbons. The relationship between these components, the ribbons, and the terms within the ribbons, is not initially clear. At a further examination it can be seen that the colour of each of the components appear in the ribbons in 2 groups, and the integrations of these components leads to the path that is needed to crate enhanced value.

The five components, Governance and Culture, Strategy and Objective-Setting, Performance, Review and Revision, Information, Communication, and Reporting in turn consist of a total of 20 different principles. Seventeen of the twenty ERM components from the 2017 Framework are discussed in the 2004 Framework though, not in nearly as much detail. Components 9 (Formulates Business Objectives) & 11 (Assesses Severity of Risk) have subtopics that are not included in the 2004 version, whereas the concepts included in Component 8 (Evaluates Alternative Strategies) are not addressed almost at all. Regardless of the similarities of the two frameworks, the depth of the discussions is not equal. The new framework places focus on the principles of Governance & Culture and Strategy & Objective-Setting as these two principles require an increased ERM

responsibility to the highest levels of management and create an ERM (Prewett & Terry, 2018). The comparison between the components of the latest 2 version can be found in the table below:

Table 5 Comparison of 2004 & 2017 ERM Frameworks

2017 Component	2017 Principle	2004 Component	Comments
Governance and Culture	1. Exercises Board Risk Oversight	Internal Environment	
	2. Establishes Operating Structures		
	3. Defines Desired Culture		
	4. Demonstrates Commitment to Core Values		
	5. Attracts, Develops, and Retains Capable Individuals6. Attracts, Develops, and Retains Capable Individuals		
Strategy & Objective-Setting	6. Analyses Business Context	Objective Setting	
	7. Defines Risk Appetite		
	8. Evaluates Alternative Strategies		Most key concepts missing
	9. Formulates Business Objectives		Some key concepts missing
Performance	10. Identifies Risk	Event Identification	
	11. Assesses Severity of Risk	Risk Assessment	Some key concepts missing
	12. Prioritizes Risks	Rik Response & control Activities	
	13. Implements Risk Responses	Risk response	
Review and Revision	14. Develops Portfolio View	Monitoring	
	15. Assesses Substantial Change		
	16. Reviews Risk and Performance		
	17. Pursues Improvement in Enterprise Risk Management		
Information, Communication, and Reporting	18. Leverages information and technology	Information and communication	
	19. Communicates risk information		
	20. Reports on risk culture and performance		

2.5.3. Comparison of ISO and COSO ERM frameworks

Different risk management frameworks often have different structures, requirements, and terminology. In this section a comparison will be made of the two most prevalent risk

management frameworks, ISO 31000 and COSO ERM (2017), by bringing the models in common ground and highlighting their similarities and discrepancies.

Starting with the common aspects, none of them are certifiable as both serve more as guidelines for the practitioners. Especially ISO 31000 aims to provide guidance on the components of a risk management framework. Since risk management should be tailored to each organization, it is only logical that the standards are really guidelines. It is up to each company to implement the guidelines, based on their cultural aspects and their needs. The universal application is also helped by the fact that both frameworks have been updated within the last three years, so they have adapted to meet the current market needs and simplified their understanding and implementation, even though the ISO 31000 states that it is not intended to promote uniformity of risk management across organizations (Rubino, 2018).

When looking in the aims and scope of the two frameworks strong similarities can be found. Both expand the scope of risk management to encourage organisations to take risks rather than just trying to limit negative impacts, thus increasing the value created. They also embed risk management in the decision-making process, which is needed to ensure that the organisation is taking the right risks in the right amount. The importance of this is highlighted by both documents.

The differences between ISO 31000 and COSO naturally outnumber the similarities. These can be the descending factors for organizations on which standard they have chosen. The biggest differences can be summarised in the bellow points (Wiliams, 2019):

1. General structure: Since ISO 31000 is created by an international standards organization, it is expected to have a more standardized structure. The standard can be read easily and quickly as it has only 26 pages. COSO has more than 200 pages and does not adhere to any kind of common “structural” pattern, but it includes more visual resources provides a greater level of detail regarding the principles and focus points.
2. Focus: Because of its origins in audit and internal control, COSO focuses more on corporate governance. While ISO focuses almost exclusively on risk and incorporating it in the strategic planning process. It also provides more specific inductions to help Top Management to better define and fulfil their risk oversight responsibilities.
3. Target: Even though the 2017 version of COSO has a greater emphasis on strategy, it can be argued that the standard is more focused on accounting and auditing purposes, thus it was designed to meet auditing needs. On the other

hand, ISO 31000 can be used by anyone interested in risk management. Since it is fully compatible with other ISO standards that could already be in use, many organizations end up opting for ISO 31000.

4. Writing process: ISO, as stated by its name, is an international organisation so the standards issued by the organisation are created with the contribution of many countries around the world. In the case of ISO 31000 people from more than 70 countries commented on it before its review in 2018. Contrary, COSO is a USA based organisation and their standard was developed in partnership with PwC, one of the "Big Four" accounting and consulting firms and almost all principal contributors for the latest update were in USA.
5. Risk appetite: The 2017 version of COSO goes into great detail regarding the concepts of risk appetite, tolerance, and capacity and also presents many visual examples. In the initial version of ISO 31000 (2009) none of the above concepts were mentioned at all. The recent version only briefly mentions the topic of risk "criteria" and uses different terminology than other resources.
6. Value: ISO 31000 places more emphasis on helping organizations accomplish their goals rather than simply avoid negative outcomes of risks. It is perceived that COSO's 2017 update it is encouraging risk "hunting" or more precisely is risk-centric, even though it focuses more on achieving objectives.
7. Structure and processes: The ISO standard provide a clear distinction between the concepts of framework and process. While the process outlined is quite simple, it goes into detail on the actual elements of risk identification, and assessment. COSO combines these two concepts. but the framework mentions the actual process of risk management only in one component.

Table 6 Comparison of ISO 31000 and COSO ERM 2017 frameworks

Stages of ERM	**ISO 31000**	**COSO ERM 2017**
Understanding the organization and its internal and external context	Establishing the Context	Governance and Culture Strategy and Objective-Setting
Risk management activity	Risk assessment	Performance
Control activities and monitoring	Risk treatment Monitoring and review	Review and Revision
Information and communication	Communicate and consult Recording and reporting	Information, Communication and Reporting

Adapted from (A Comparison of the Main ERM Frameworks: How Limitations and Weaknesses can be Overcome Implementing IT Governance, 2018)

This is only a brief overview of the similarities and differences between the two proposals since a detailed analysis would be needed to cover everything. It cannot be stated that either approach is universally better the other as this depends on the organization it is applied to, its needs, its culture, the maturity, its structure and so on. The implementation of an enterprise risk management system is a very complex activity, and many factors should be considered before deciding what approach will be followed.

3. Methodology

3.1. Introduction

This chapter presents the research methodology and approach that is used to perform the survey. With the deployment of a questionnaire, this thesis will attempt to assess the Enterprise Risk Management implementation in the Greek market. The questionnaire has been distributed to over 5000 companies across Greece, from a variety of fields and sizes. According to the answers received and the use of a maturity model, each company will be graded with an implementation rank, the sum of which will be investigated. Based on the answers the thesis will attempt to quantify the risk appetite of Greek companies as well as highlight the use of the most common business tools related to the ERM.

3.2. Sampling method

From the five main ways to collect the data needed, meaning observation, interviews, focus groups and questionnaires the latter was selected. Given the subject it was considered the best option, as it provides the opportunity to carefully structure and formulate the data collection plan with precision and allows the participants to fill them at a convenient time and think about the answers at their own pace. Also, a questionnaire sent by email can reach companies all around Greece in the shortest amount of time.

The mailing list was provided by the University of Piraeus and consisted of 6260 companies from all over Greece. Apart from the contact information and the field of business no economic or size indicators were available, so no filtering was on the provided list. All were sent in the span of approximately one month, and the end of the survey was set at two weeks after the final questionnaire was sent. The email sent can be found in Annex 2.

As expected, the response rate was very low. From the 6260 questionnaires sent only 98 valid answers were received amounting to a 0.15% rate of response. Along with the risk of not being able to verify the participants, low participation are the biggest downsides of this method.

3.3. Development of the questionnaire

The questionnaire was created with the on Google forms for the ease of use that it provides. Even though it was addressed to the Chief Executing Officer, Members of the Top Management of the Risk Manager, to further assist the participants as much as possible, the choice was made for the questionnaires to be made in Greek. Given the wide diversity of the recipient backgrounds, familiarity with the topic and general business term knowledge the use of the Greek language was preferred (with the addition of some terms in English when considered necessary). The full questionnaire can be found in Annex 1.

In the introduction of the questionnaire a brief introduction was placed mentioning the topic of the survey, the authors identity and contact information, the supervising professor, and of course the university and Its logo.

The selected 25 questions can be grouped in 6 different groups:

1. Questions 1-4 & 21-25
   This group consists of mostly demographic and general questions, aiming to collect data regarding the size, field of business and the role of the person answering in the company. Two questions can also be found in this group regarding the recent COVID-19 pandemic, since it is a recent risk worth looking into.
2. Questions 5-12 & 14
   This group, and each of the three following relate to the basic concepts of ERM. Starting with the understanding of the context and basic structures, the questions of this group aim to identify the organisation of each company, the scope of the ERM and their risk appetite.
3. Question 13
   Question 13 consists of a matrix with a 5-point Likert agreement scale, measuring the existence and integration of risk identification structures. In order to assess the integration level, the participants were asked to select how easily and quickly a newcomer would recognise the risk identification, assessment, prioritisation, etc. structures existing in the company.
4. Questions 15-16
   Risk treatment methods and their efficiency are not easy to quantify at this scale with the use of a general questioner. With this limitation the questions of this

group focus on the frequency that Top Management takes into amount the outcomes of ERM and plans actions for specific risks.

5. Questions 17-19

   These questions are related to the last concept of ERM, communication and monitoring. In this group the frequency of the review of the ERM is requested as well as if there is a dedicated way of reporting the outcomes of the ERM.

6. Question 20

   Question 20 focuses on common busines tools that can be used by any company to assist in the ERM implementation. Again, with the use of a matrix the participants were asked to fill in their affiliation and knowledge with specific types of tools, and if they are used in the company.

3.4. Data analysis

Due to the simplicity of the data collected, Microsoft Excel was chosen as the tool for visualisation and analysis. In order to better depict the answers basic techniques were sues in the lines of grouping of similar answers, counting the frequency of each answerer or calculation the selection of each answer in percentages.

To evaluate the maturity of level of the companies regarding the ERM the author used a maturity model which is a way to show how capable an organization or system is of achieving continuous improvement in a particular discipline. Various maturity models exist depending on the topic examined, so for the implementation of ERM the Capability Maturity Model was selected (Paulk, Curtis, Chrissis, & Weber, 1993). Maturity level defines the degree of formality and optimization of a processes, from ad hoc practices, to formally defined steps, to managed result metrics, to active optimization of the processes. The main purpose of the model was to improve existing software development processes, but it can be more broadly applied to a range of processes.

The maturity levels are:

- Level 1 – Ad hoc
- Level 2 – Repeatable
- Level 3 – Defined
- Level 4 – Capable
- Level 5 – Efficient

3.5. Profile of the participants

From the 98 replies, the vast majority were answered by the CEO of the company or an equivalent role, and 42% belonged to a larger organization or group. Further information regarding the profiles of the participants follow.

3.5.1. Business fields

Most answers were received from companies working in ether the food (15), trade (12) or construction (10) sectors, as seen the bellow table. Even with some singular entries, participation from more than 25 different fields has been achieved.

Table 7 Business field of the participants

Business Field	**No of replies**
Food	15
Other	13
Trade	12
Construction	10
Crafts	5
Internet services	5
Transportation	5
Energy industry	5
Finance	3
Computer software and applications	3
Telecommunications	2
Industry	2
Health services	2
Engineering	2
Chemicals	1
Agriculture	1
Restaurants	1
Shipping	1
Public services	1
Clothing and textiles	1
Livestock	1
Arts	1
Pharmaceutical	1
Petroleum and natural gas	1
(Blank)	4

3.5.2. Years in operation

61% of the participants were in operation prior to the year 2000. From there, in increments of 5 years a similar distribution can be noted, with the exception being the “1 – 5” bracket (6%).

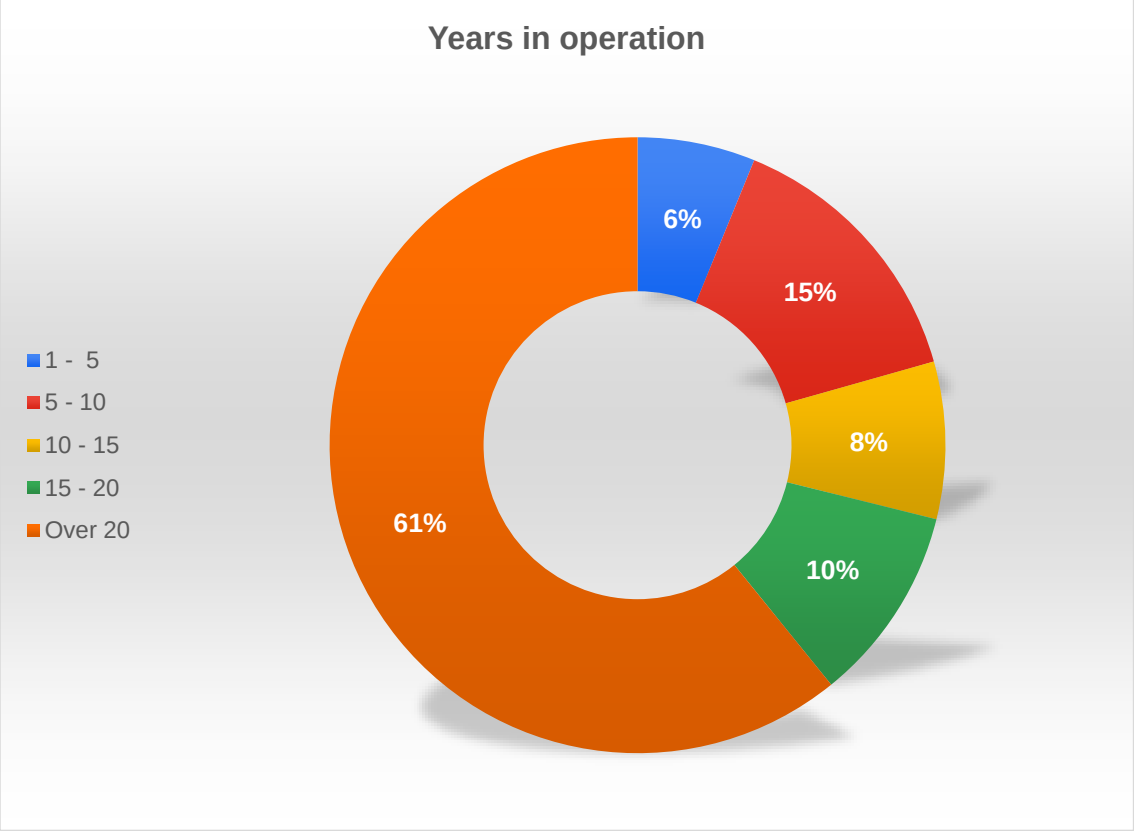


Figure 6 Years in operation for the participating companies

3.5.3. Number of employees

Regarding the size of the companies in terms of employees, a close to even distribution can be found skewed a bit toward first two brackets, with the companies employing up to 24 people consisting of 41% of the sample size.

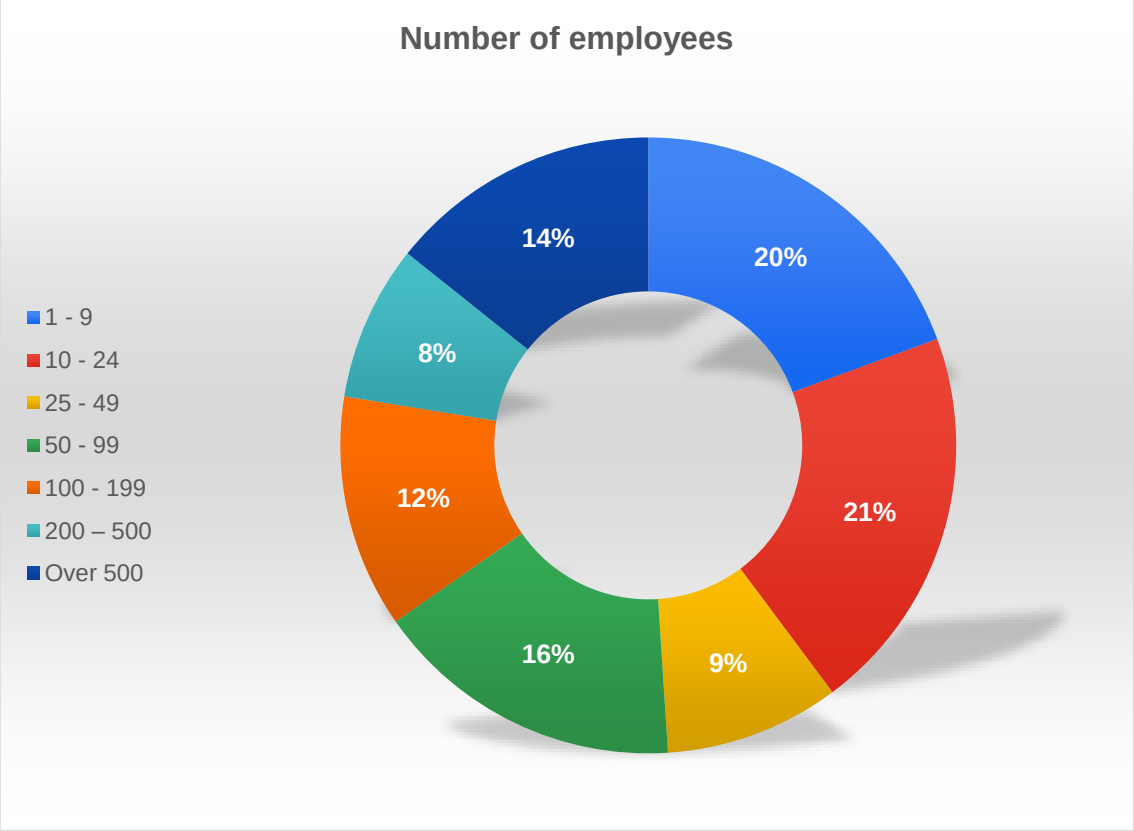


Figure 7 Number of employees of the participating companies

3.5.4. Turnover

The majority of the participants (27%) reported that in 2019 had a turnover between 1 and 5 million €. The second largest percentage is the smallest bracket (up to 1 million €) with 24% followed by the highest bracket (over 40 million €). The other segments of the participants were 14% for the 20-40 million € bracket, 9% for the 10-20 million € bracket and 8% for the 5-10 million € bracket.

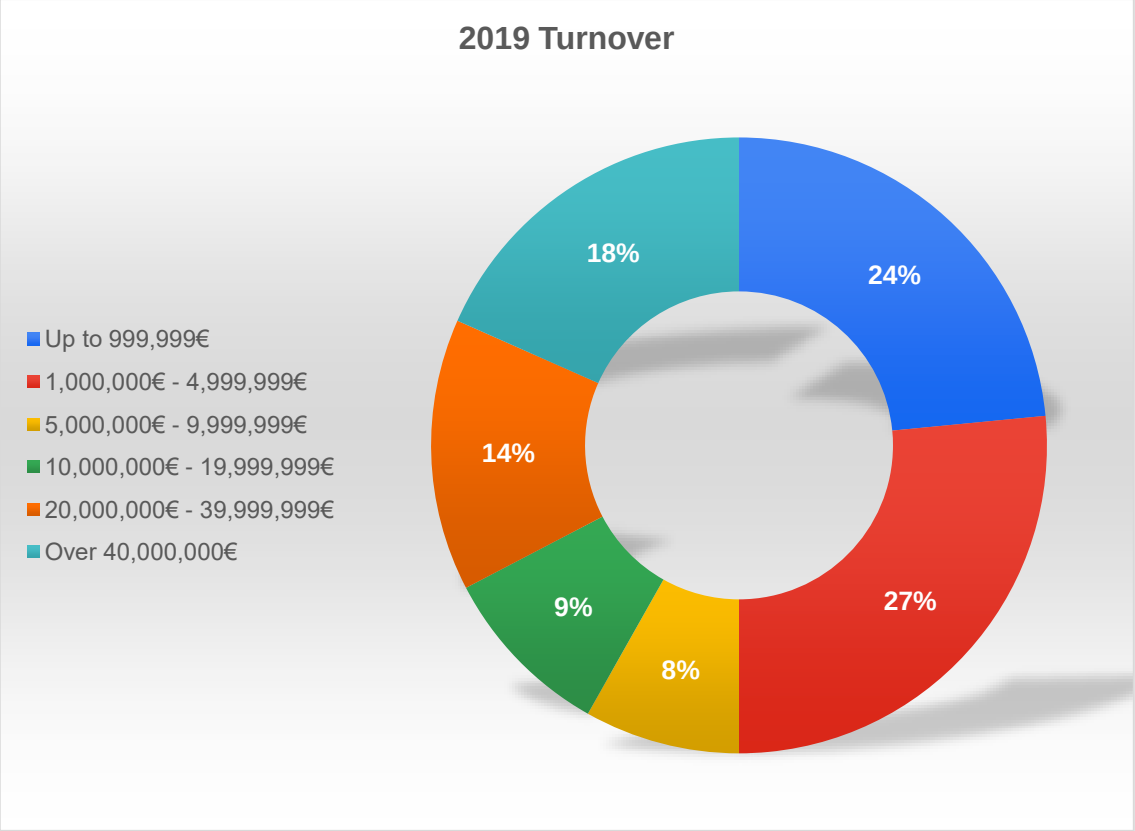


Figure 8 2019 Turnover for the participating companies

4. Data analysis & interpretation

4.1. Introduction

This chapter presents the initial survey findings on the diffusion of Enterprise Risk Management in Greek companies. The questions are grouped in six different categories:

1. General information
2. Understanding the context of the organization
3. Risk identification competency
4. Risk treatment competency
5. Communication and monitoring competency
6. Other information

The order of that the questions were organized and presented in this chapter does not necessarily align with the above 6 categories, since the questionnaire was structured in a way to be friendlier to the participants. As the general information gathered from questions 1 to 4 and 23 to 24 was presented in the previously, in this chapter the results of questions 5 to 22 will pe presented.

As expected, the response rate was quite low (1,5%), since the answers collected were only 98 from total of over 6500 questionnaires sent. Even though the survey was done at a scope covering all of Greece and the questionnaire could be answered by almost every company, It is only natural to be able to find a larger representation of the enquired structures in bigger companies.

No difficulties were observed during their completion of the questionnaires given that they were targeted to Risk Managers or members of the Top Management, however a few phone calls were made to the Author in order to clarify the content and the purpose of the survey.

The consolidation of the results and the creation of the figures was made with the use of Microsoft excel. In some questions text questions, the answers have been grouped in order to depict a more comprehensive result.

All and answers have been translated in English since the questionnaire was in Greek (Appendix A).

4.2. Results

4.2.1. ISO Certifications

Question no 5: Is the organization certified with any of the following standards?

63% of the surveyed companies had at least one of the 3 most popular ISO certifications. Most of them (58%) were certified under ISO 9001 (Quality management), followed by ISO 14001 (Environmental Management) with a percentage of 29% and lastly 13% had an ISO 45001 or OHSA 18001 certificate (Occupational Health and Safety). All three of the aforementioned standards have dedicated sections to risk management, so its is very interesting to see the correlation with ERM.

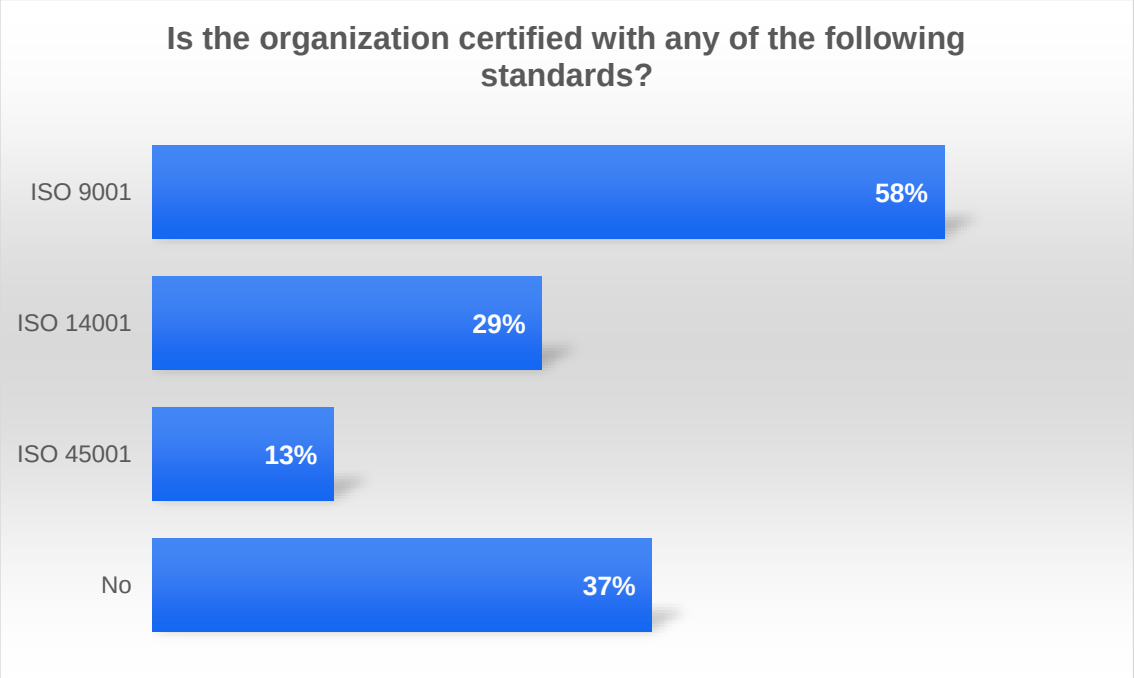


Figure 9 Response to the question: Is the organization certified with any of the following standards?

4.2.2. Enterprise Risk Management frameworks

Question no 6: Does the organization follow any specific framework Enterprise Risk Management?

The overwhelming majority (81%) of the surveyed companies did not follow any specific Framework for Enterprise Risk Management. For the ones that did, 5% followed ISO

31000, 4% followed the COSO ERM 2017 framework, 3% still use COSO's 2004 version, 2% is allocated to CAS (Casualty Actuarial Society) ERM framework and 1% is given to the BRC (Food Safety Management Systems) standard. Safety officer, Special consultant and Customer Trade Credit Insurance answers also received 1% along with the answer "I don't know".

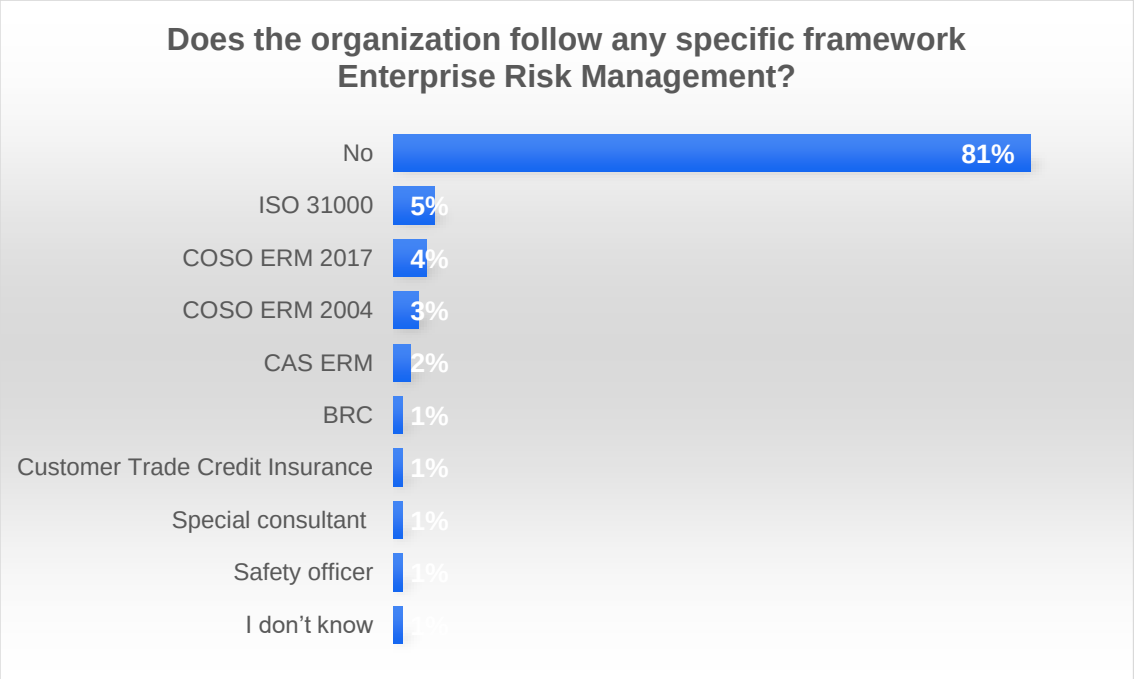


Figure 10 Response to the question: Does the organization follow any specific framework Enterprise Risk Management?

4.2.3. Risk Manager

Question no 7: Is there a dedicated role in the organization's chart relate to the ERM? If it does not exist but is managed exclusively by someone else, please fill his job role in the field "Other".

The role of Risk Manager only exists in 12% of the companies studied in the survey. In the rest of the companies that role exists but is not a dedicated position in the organization chart, ERM is managed by people in the department of Finance (4%), Quality (3%) and HR (1%), the parent company (2%), the Board of Directors (2%), the Managing Partner (1%) or it is outsourced (1%). However, the most common answer was that this ole does not exist at a percentage of 71%.

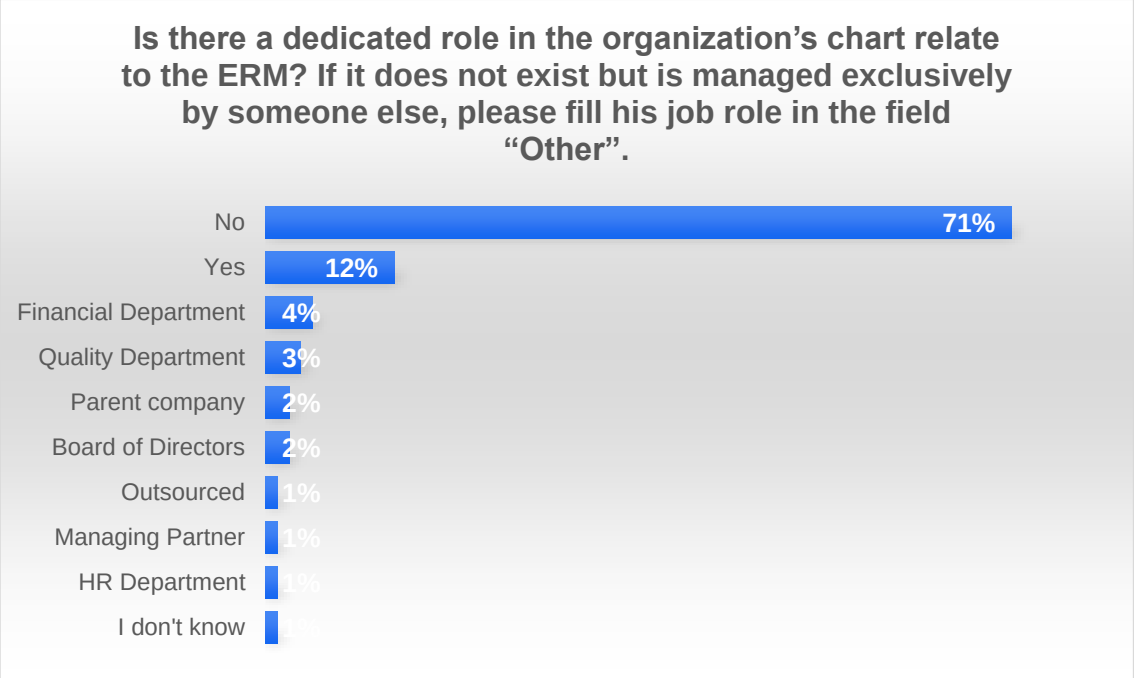


Figure 11 Response to the question: Is there a dedicated role in the organization's chart relate to the ERM?

4.2.4. General Risk Appetite

Question no 8: Which of these statements do you believe better describes your organizations approach when it comes to risk management?

The purpose of the following question is to investigate the risk appetite of the surveyed companies. Based on an adaptation of the risk appetite scales given by the UK Treasury (2006) and Rob Quail (2012), the participants were presented with 6 choices regarding their risk appetite:

1. Averse: Avoidance of risk and uncertainty is a key Organizational objective
2. Minimalist: Preference for ultra-safe business delivery options that have a low degree of inherent risk and only have a potential for limited reward.
3. Cautious: Preference for safe delivery options that have a low degree of residual risk and may only have limited potential for reward.
4. Flexible: Willingness to take strongly justified risks while expecting some level of uncertainty.
5. Open: Willing to consider all potential delivery options and choose the one that is most likely to result in successful delivery while also providing an acceptable level of reward.

6. Hungry: Eager to be innovative and to choose options offering potentially higher business rewards, despite greater inherent risk.

6% chose “Averse”, 15% “Minimalist”, 21% “Cautious”, 23% “Flexible”, 33% “Open” and only 2% chose “Hungry”.

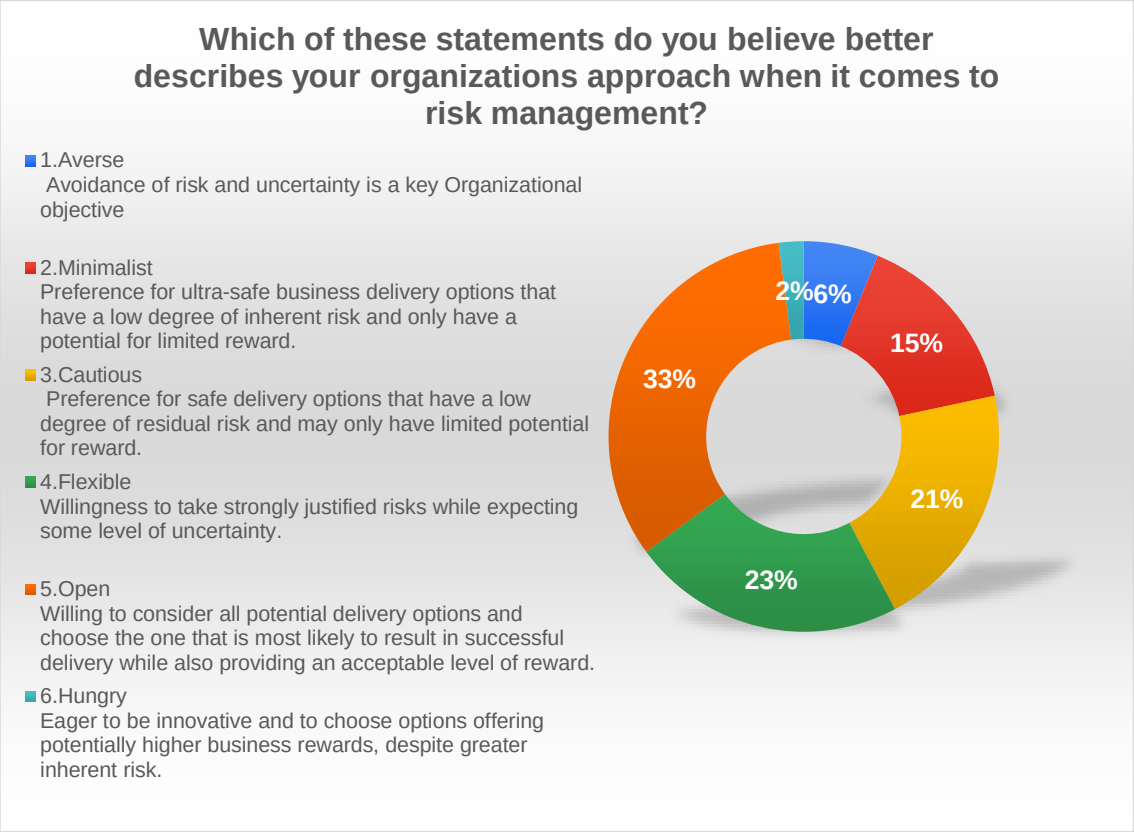
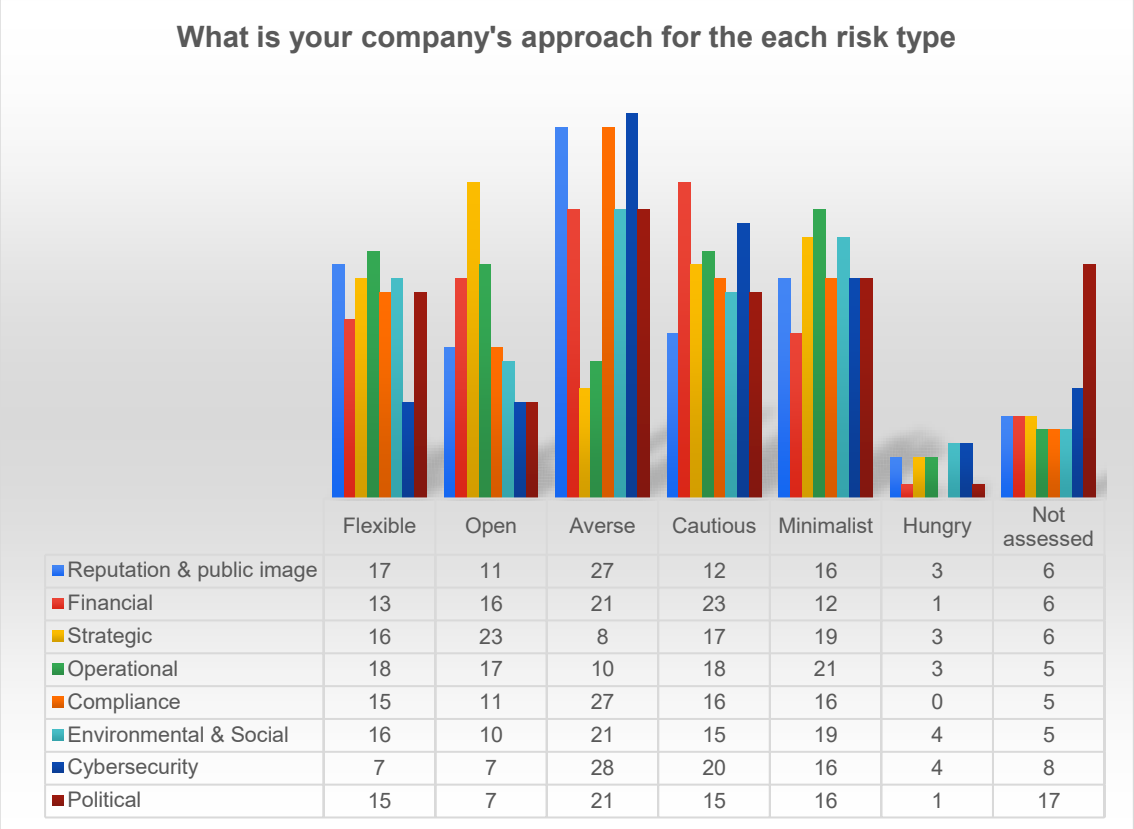


Figure 12 Response to the question: Which of these statements do you believe better describes your organizations approach when it comes to risk management?

4.2.5. Risk Appetite for specific types of risks

Question no 9: Given that every company manages differently the risks based on its nature, please fill in the table your company’s approach for each of the risk types based on the interpretation of terms from the previous question.

Having seen the overall risk appetite of the company we move forward to the approach in separate risk families. Counting the times each approach choice was selected we can see that the most popular answer was “Averse” with 163 cumulated answers, followed by “cautious” with 136, “Minimalist” with 135, “Flexible” with 117, “Open” with 102 and “Hungry” with only 19. The option “Not assessed” was selected 58 times.



	Flexible	Open	Averse	Cautious	Minimalist	Hungry	Not assessed
Reputation & public image	17	11	27	12	16	3	6
Financial	13	16	21	23	12	1	6
Strategic	16	23	8	17	19	3	6
Operational	18	17	10	18	21	3	5
Compliance	15	11	27	16	16	0	5
Environmental & Social	16	10	21	15	19	4	5
Cybersecurity	7	7	28	20	16	4	8
Political	15	7	21	15	16	1	17

Figure 13 Response to the question: Fill in your company's approach for each risk type

4.2.6. Scope of the ERM (Turnover)

Question no 10: At what percentage of the annual turnover (percentage of customers) the organization applies ERM?

37% of the participants reported that the ERM is applied only up to 19% of the company's turnover or customers, which may include the possibility of the no implementation of ERM at all. Up to 39% received a 14%, up to 59 received a 18%, up to 79% received a 9% and up to 100% received 23%.

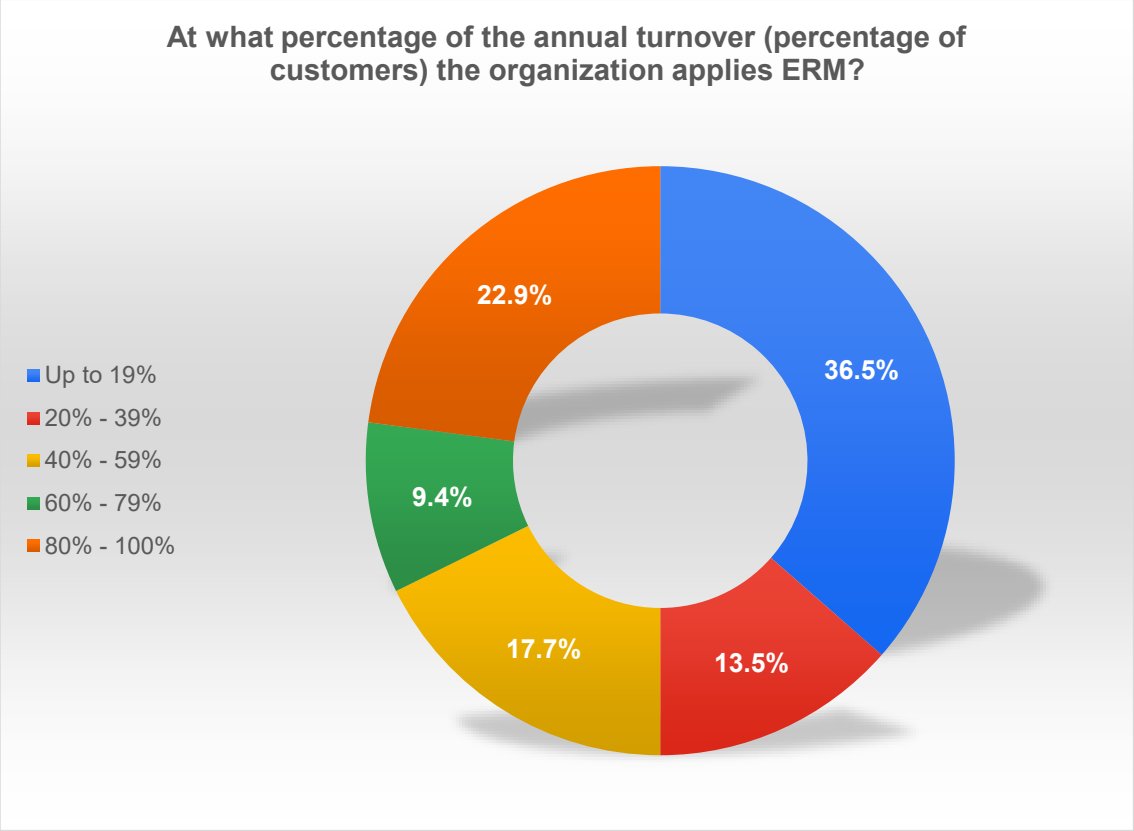


Figure 14 Response to the question: At what percentage of the annual turnover (percentage of customers) the organization applies ERM?

4.2.7. Scope of the ERM (Processes)

Question no 11: In which of the organization's processes is the ERM applied?

Given the origins and sometimes the interpretation of ERM, it is expected to see that the process in which the ERM is most consistently applied is Finance (68%) followed closely by Accounting and Sales (58%) and of course Management (57%). Near the 50 % mark we find Quality and improvement and near it Legal (48%), Information Technology (47%), Customer Support / After Sales (46%), Supply Chain (43%), Marketing (42%) and Product Development (39%). The lowest percentages are found in the processes of Human Resources (34%) and Research & Development (29%).

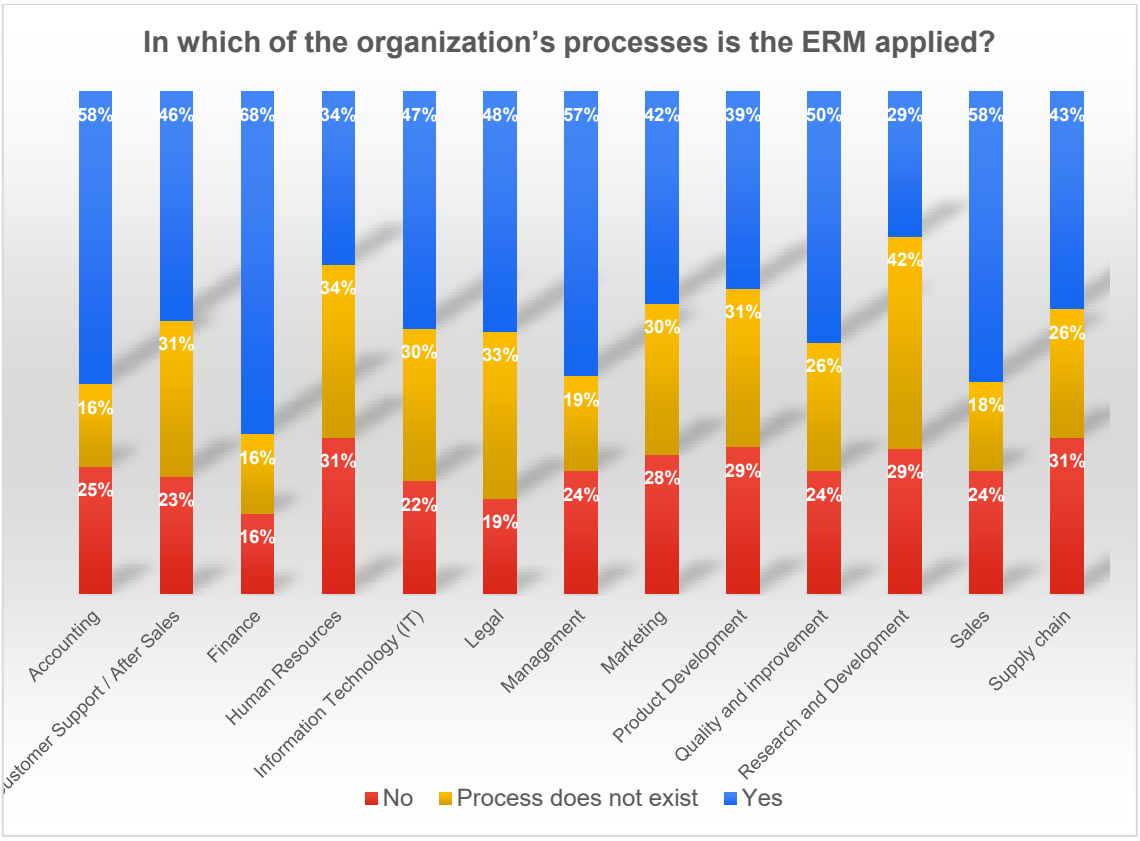


Figure 15 Response to the question: In which of the organization's processes is the ERM applied?

4.2.8. Established performance tracking (Key Performance Indicators)

Question no 12: In which of the organization's processes are there specific and quantified objectives and tracking?

Continuing form the question 11, the aim of this question is to define if there are established goals and objectives in the company and if the management is able to track their status. Similarly to Figure 13, We find the presence of performance tracking in Finance (70%) and Sales (69%) leading the answers but after that there is a big gap between them and the next process which is Customer Support (59%). Starting form the biggest percentage the rest of the processes are Management (56%), Marketing (53%), Quality and improvement (52%), Accounting (47%), Product Development (45%), Supply chain (43%), Information Technology (38%), Research and Development (31%), Human Resources (30%) and Legal (24%).

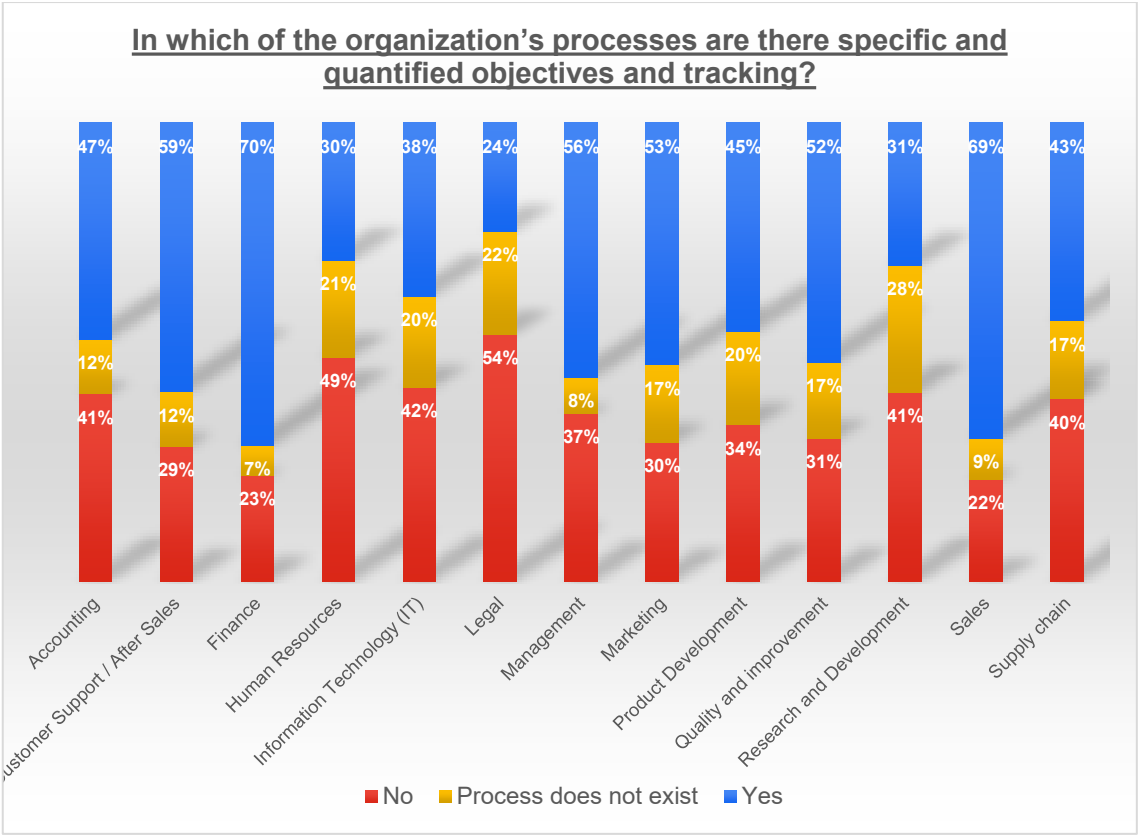


Figure 16 Response to the question: In which of the organization's processes are there specific and quantified objectives and tracking?

4.2.9. Established structures and procedures related for the ERM:

Question no 13: If a new member arrives, how quickly and easily will he ascertain that in the organization the following structures are established

In order to investigate the extent in which the ERM is integrated in the company's organization, the viewpoint of a newcomer was requested. The questions relate to some of the core aspects of ERM: Structures and Roles, Risk Identification, Evaluation, Prioritization & Recording, and Input method for monitoring the company's environment. Using a 5-point Likert scale, we see that for the majority of the aspects, most answers tend to be on the negative side with the exceptions being the existence of procedures of risk identify and change monitoring as seen in figure 17

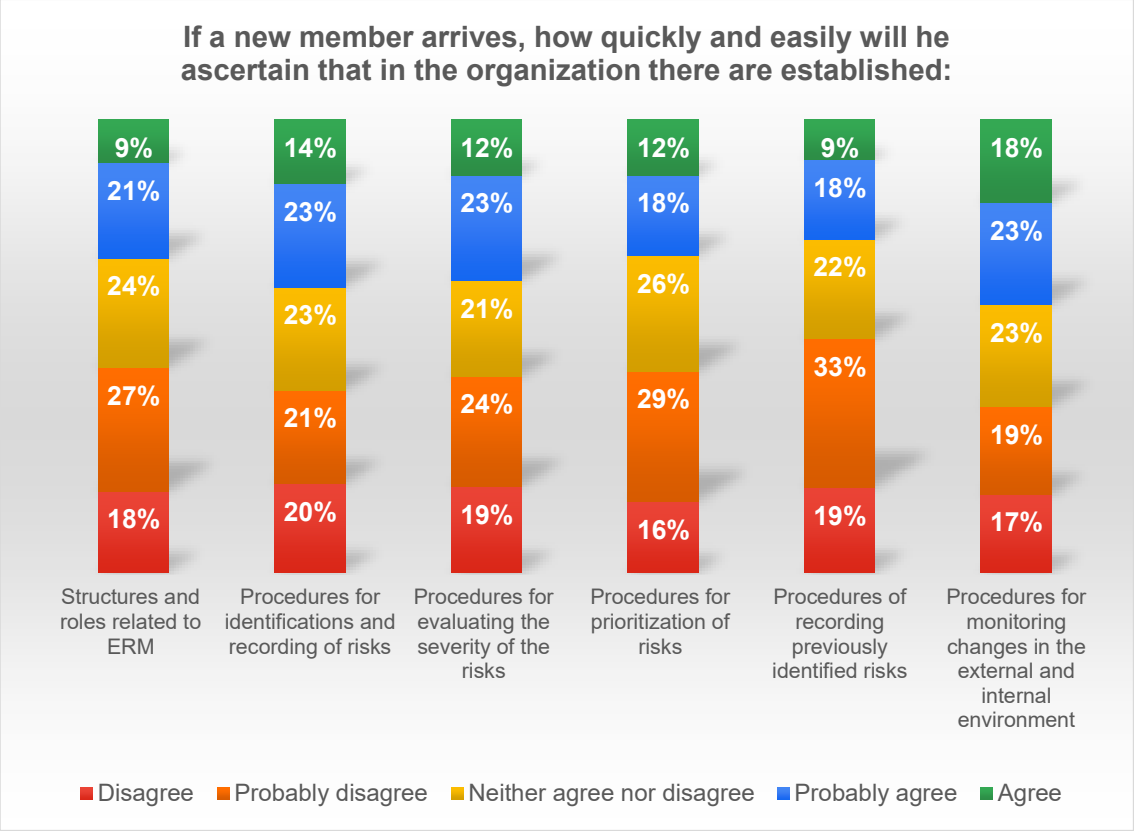


Figure 17 Response to the question: If a new member arrives, how quickly and easily will he ascertain that in the organization selected core aspects of ERM are established

4.2.10. Provision of resources for ERM

Question no 14: In what way does Top Management distribute resources (material and manpower) for the ERM?

In order to discover if there is a systematic distribution of resources for the ERM, question 14 referred to the frequency Top management does so. 33% answered that the is no specific distribution, 34% that it is done according to the situation, 18% that it is a part of each process plan, 13% that it is a part of the annual plan and only 2% that it is done formally, with a higher frequency of once per year.

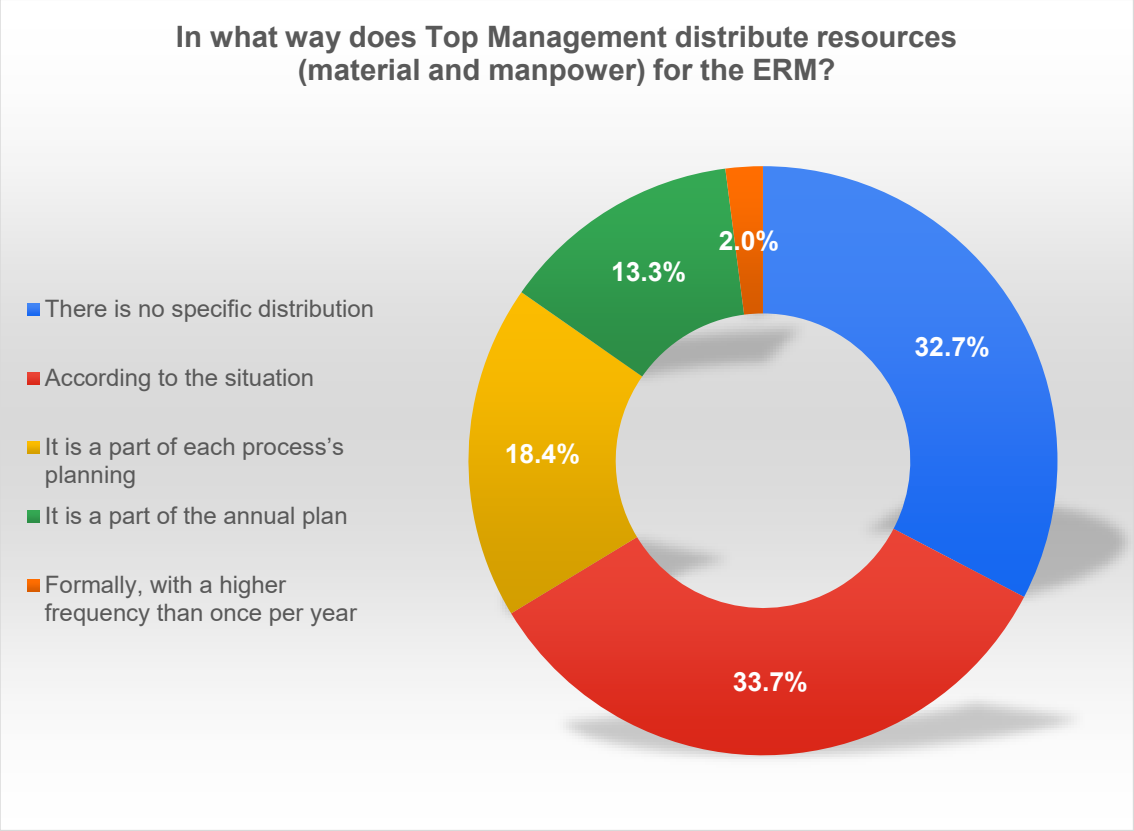


Figure 18 Response to the question: In what way does Top Management distribute resources for the ERM?

4.2.11. Inclusion of the ERM outcomes in the decision-making process

Question no 15: How frequently does Top Management include the results of ERM in the decision-making process?

In continuation to question 14, in this question the participants we asked to answer how frequently Top Management includes the results of ERM in the decision-making process. Starting with the highest frequency, 23% chose “Always”, 31% chose ”Often”, 37% chose “Sometimes – When needed” and 9% chose the option “Rarely”. The option “Never” was not chosen by any of the participants.

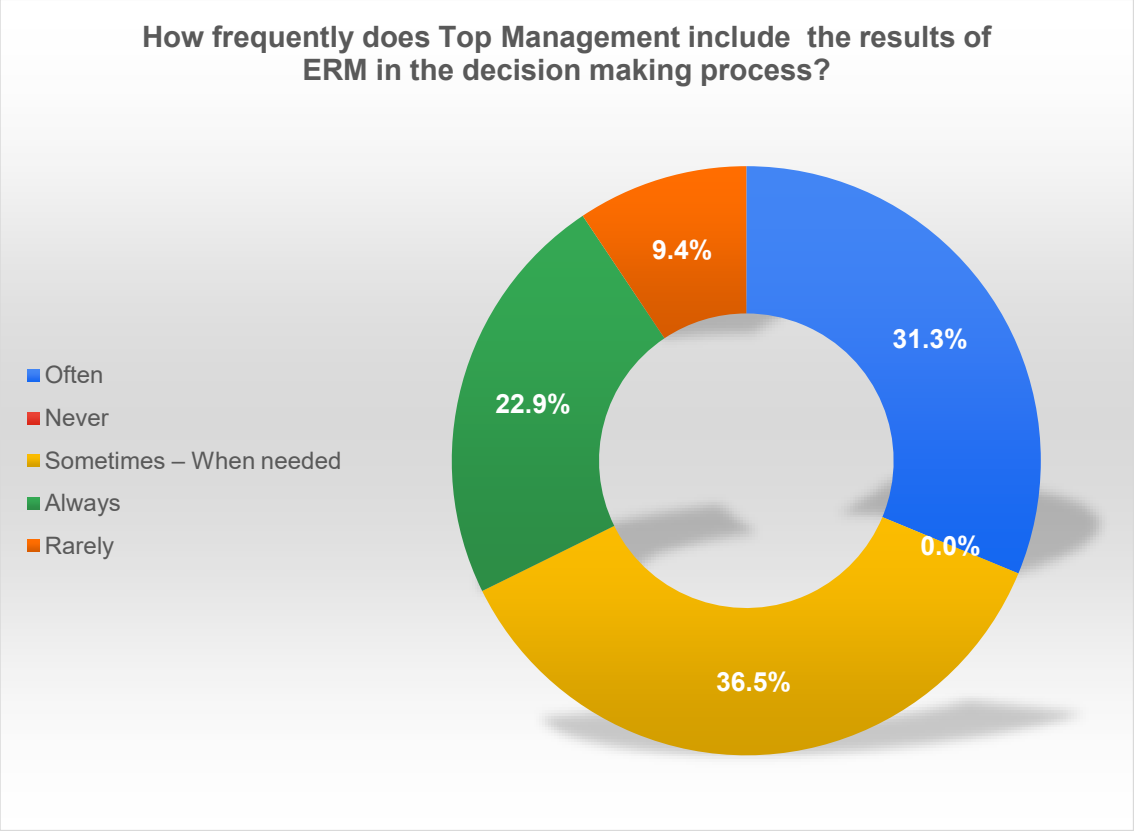


Figure 19 Response to the question: How frequently does Top Management include the results of ERM in the decision-making process?

4.2.12. Action setting for selected risks

Question no 16: How often does Top Management sets specific actions for identified risks?

Staying in the same topic, question 16 refers to the risk response actions. Using the previous scale we see that 9% chose “Always”, 24% chose ”Often”, the majority with 51% chose “Sometimes – When needed”, 14% chose the option “Rarely” and 2% even chose the option “Never”.

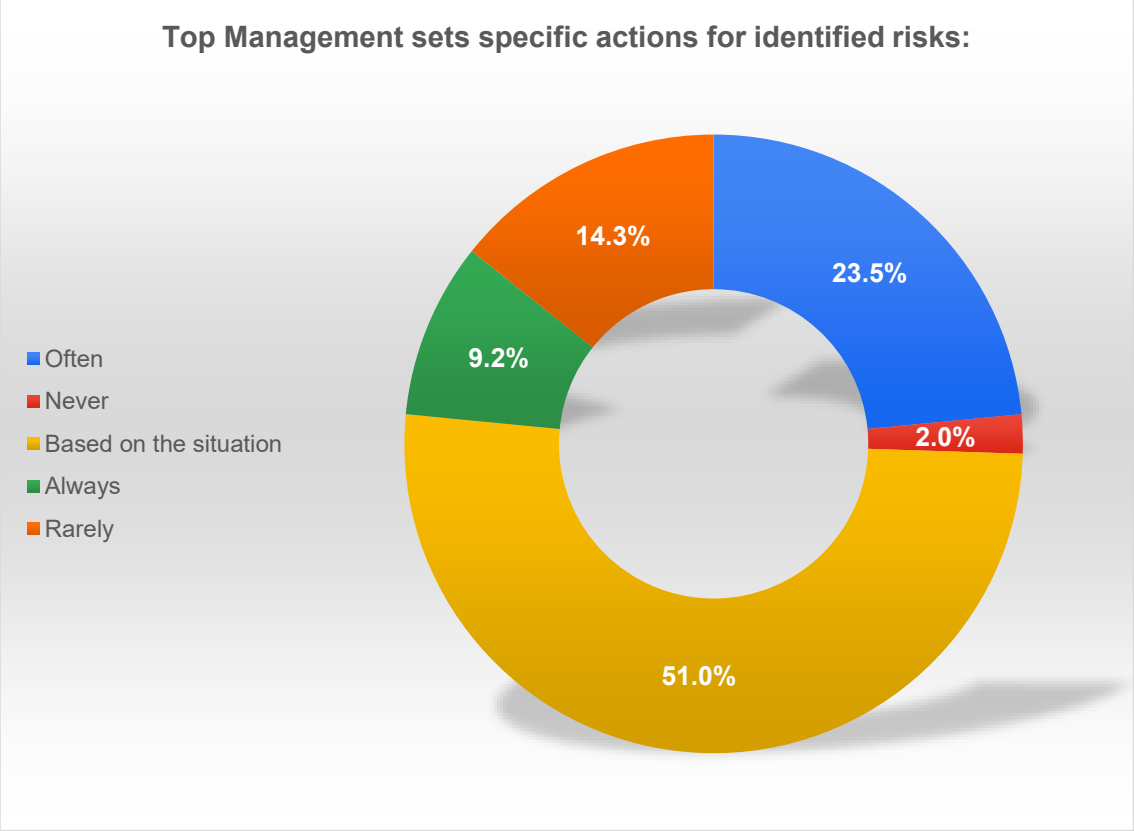


Figure 20 Response to the question: How often does Top Management sets specific actions for identified risks?

4.2.13. Review of the effectiveness of the actions set

Question no 17: How often does Top Management review the outcomes of the actions taken for specific risks?

The next step after the action setting and implementation is the review of their effectiveness. With the use of a more specific frequency scale, 6% reported that the review is done on a monthly basis, 16% at least every 3 months, 18% at least every 6 months, 14% at least every year, however most participants 46% reported that this review is done “when needed”.

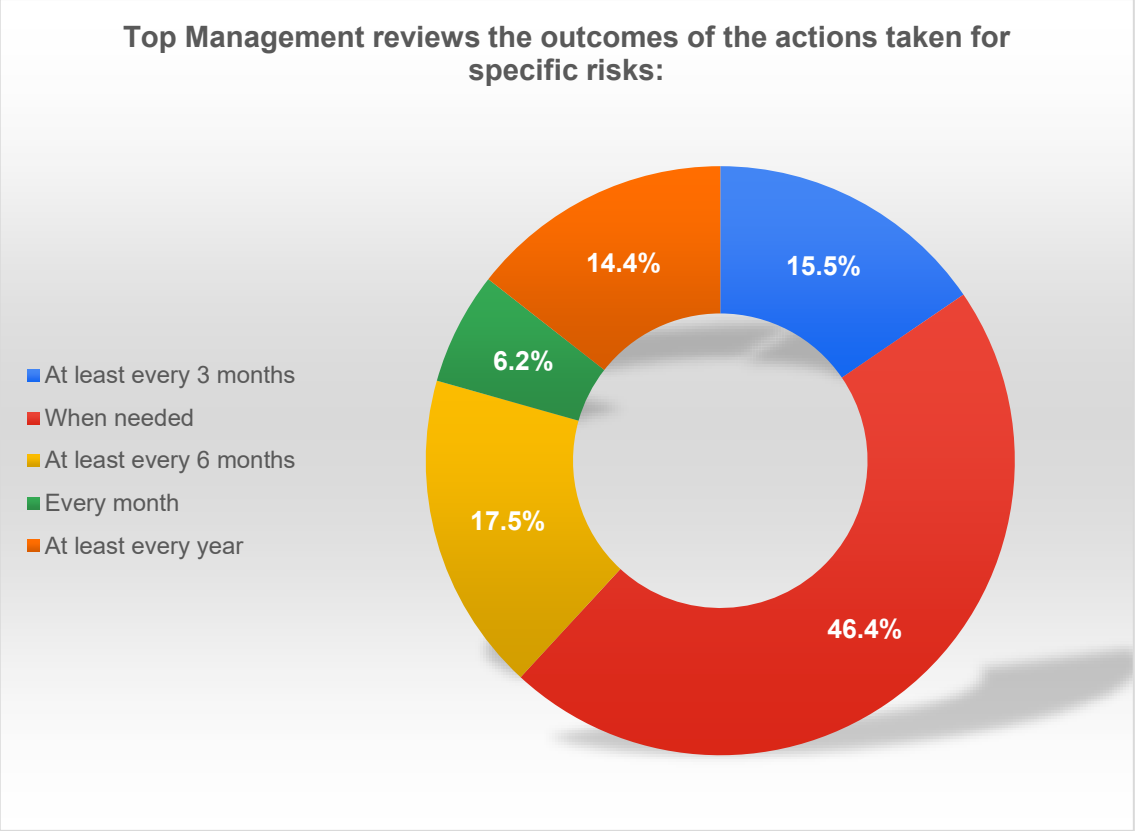


Figure 21 Response to the question: How often does Top Management review the outcomes of the actions taken for specific risks?

4.2.14. ERM performance review

Question no 18: How often does Top Management review the performance of ERM?

The effectiveness of the actions set is an entirely different concept from the performance of Enterprise Risk Management system in place. According to the results of the survey this is done mostly (51%) “When needed”. The participants who selected specific timeframes chose mostly “at least every 6 months” (20%), followed by “at least every year” (18%) and equally (6%) “at least every 3 months” & “Every month”,

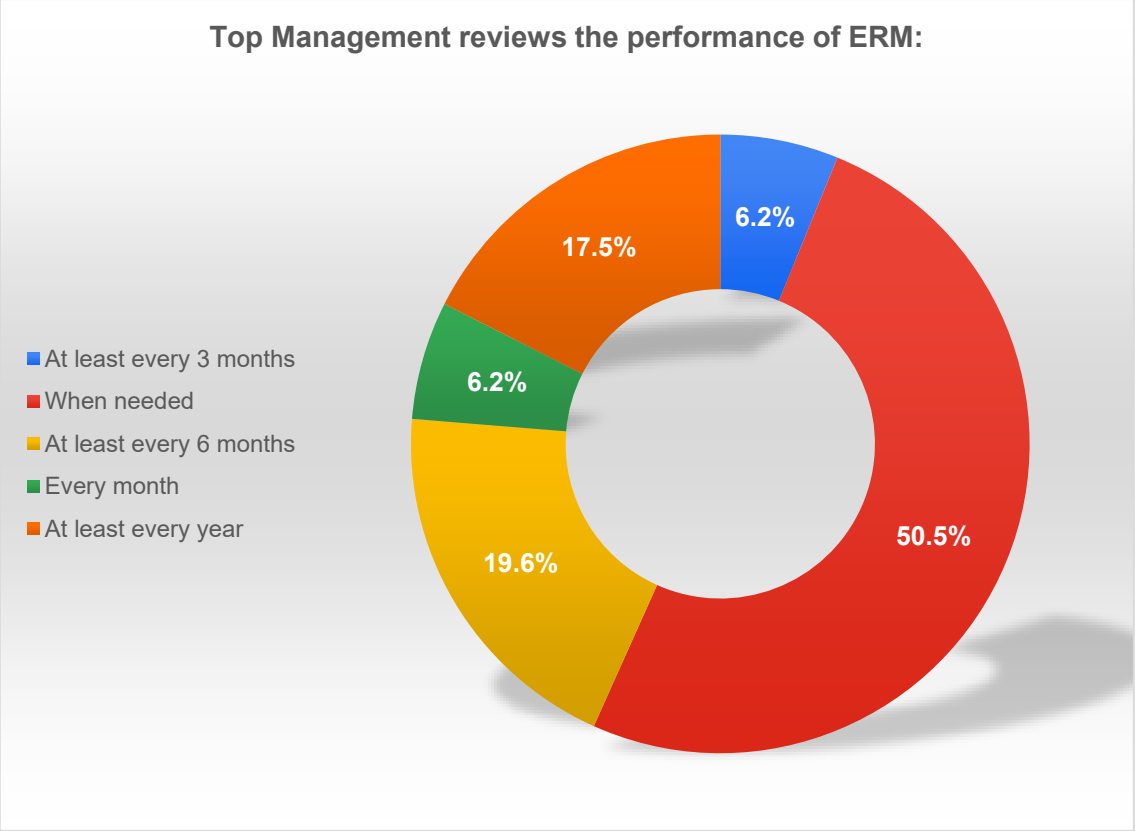


Figure 22 Response to the question: How often does Top Management review the performance of ERM?

4.2.15. ERM reporting to Top Management

Question no 19: Is there a dedicated procedure regarding the ERM reporting to the Top Management?

The final question regarding the Top Management is regarding the ERM information and reports. The question asked is if a specific reporting procedure regarding the outcomes of ERM exist at which 71% responded negatively.

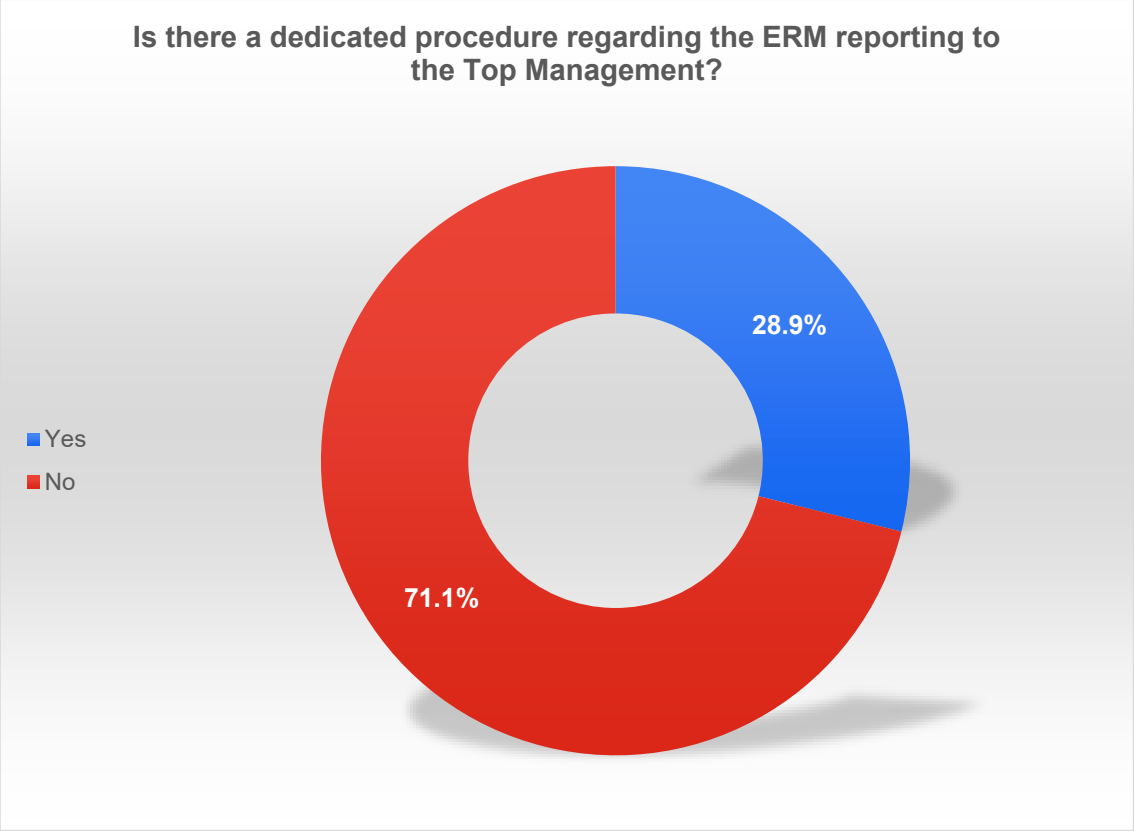


Figure 23 Response to the question: Is there a dedicated procedure regarding the ERM reporting to the Top Management?

4.2.16. Busines and ERM tools

Question no 20: Fill in your affiliation with the presented business tools

The process of risks management is very complex, and several tools can be used to facilitate it. Question 20 revolves around some tools that can be used by a company in order to assist in the application of some core aspects of ERM and risk management in general. The 14 tools (or practices) used in the survey in broad strokes can be separated in 6 categories, even though many of them can be included in more than 1.

- Transversal
    - Formalized management review
    - Quality tools (i.e.6 sigma, Pareto)
    - Systemic feedback from the employees
    - Cooperation with external consultants
- Gathering of Input
    - Surveys regarding the organization's public image

    - Customer satisfaction surveys
    - Subscriptions to media outlets
    - Systemic updates for changes in the legislation
    - Systemic updates for changes in the tax legislation
    - Participation in forums concerning the core business
- Data analysis
    - ERP software
    - Business intelligence software
- Risk analysis
    - Risk matrixes
- Risk treatment
    - Cybersecurity software

The participants we asked to provide their (and in extension, their company's) affiliation with these tools, and the results are presented in Table 8.

Table 8 Response from the question: Fill in your affiliation with the presented business tools

	I have heard of it	I am aware of it, but it is not used	It has been used in the past	It is used frequently
Risk matrixes	26	34	13	20
Surveys regarding the organization's public image	19	34	25	17
Customer satisfaction surveys	11	28	20	34
ERP software	12	22	7	52
Business intelligence software	23	43	7	21
Subscriptions to media outlets	13	20	22	41
Cybersecurity software	9	8	9	68
Systemic updates for changes in the legislation	15	19	13	47
Formalized management review	16	30	16	32
Quality tools (i.e.6 sigma, Pareto)	31	44	7	12
Systemic updates for changes in the tax legislation	12	17	21	44
Participation in forums concerning the core business	11	26	23	34
Systemic feedback from the employees	12	25	28	29
Cooperation with external consultants	15	26	19	34

If we visualize the data from table 8 and use percentages, we can easily see the popularity of the tools, for example, 72% is frequently using cybersecurity software whereas only 13% any quality tools such as Pareto diagrams.

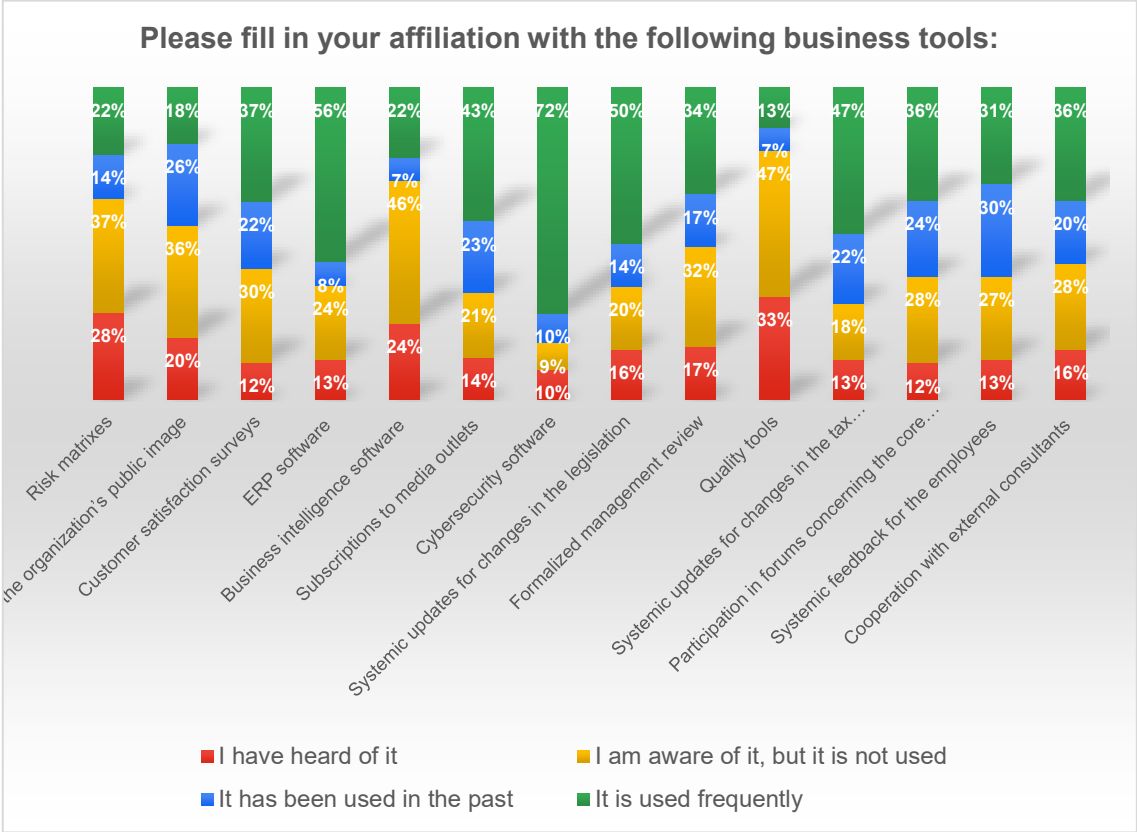


Figure 24 Response to the question: Fill in your affiliation with the presented business tools (percentages)

4.2.17. Covid -19 Health Crisis

Question no 21: How satisfied are you with the management of the health crisis of COVID 19 by your organization?

&

Question no 22: Has your organization already set specific actions for the management of the existing and future COVID 19 related risk affecting the organization?

Given the time the survey took place, It was interesting to see how the surveyed companies dealt with a new risk, the global health crisis of Covid-19. With that in mind the above two questions were asked and the feedback received was very positive. On a satisfaction scale from 1-5 regarding the overall management of the crisis by their company, 50% answered 5, 33% answered 4, 13% answered 3, 13% answered 2 and only 3% answered 1%.

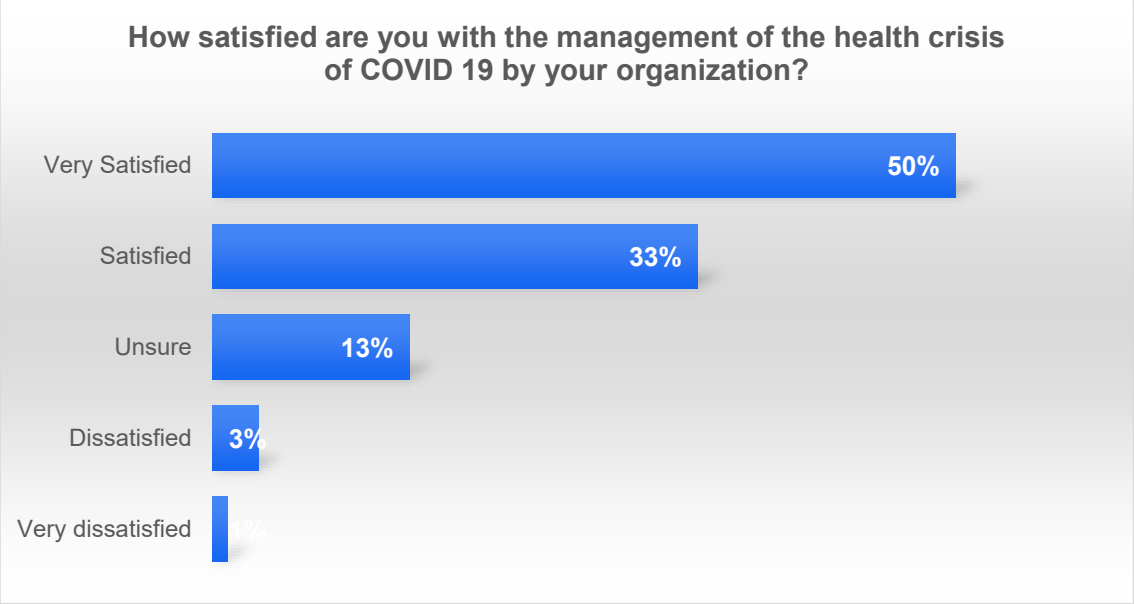


Figure 25 Response to the question: How satisfied are you with the management of the health crisis of COVID 19 by your organization?

Furthermore, 77% reported that they have already planned actions to address existing and possible risks related to the pandemic.

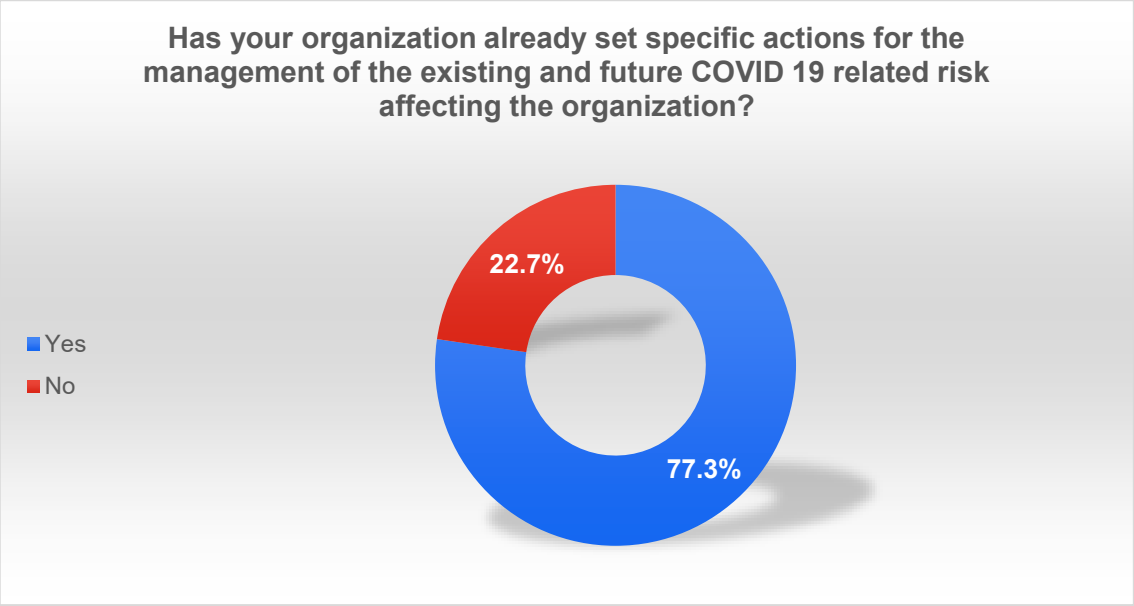


Figure 26 Response to the question: Has your organization already set specific actions for the management of the existing and future COVID 19 related risk affecting the organization?

5. Conclusions

5.1. Introduction

The purpose of this survey was to investigate the depth of the diffusion of enterprise risk management in Greek companies. Based on the review of the most relevant literature, including books, publications, and the most prevalent frameworks, a questionnaire was launched whose received answers were presented in the previous chapter.

This final chapter begins by analyzing the outcomes of the survey and presents a brief conclusion. Closing, the limitations of the thesis are described, and the author gives his suggestions for practitioners of ERM and proposals for further research on the subject.

5.2. Analysis of findings

This thesis was driven by a set of research questions which are revisited in this section. In order to provide answers to these questions, a simple analysis and interpretation of the data collected has to be done. The three main questions are the following.

5.2.1. What is the level of diffusion of ERM in Greek Companies?

The quantification of how well developed the ERM process is in a company, is quite difficult. The application depends on many different factors for each company, so unless a thorough investigations, or audit is done in each of them, there cannot be a full proof answer. In order to tackle this issue for the purposes of this survey, based on the basic concepts of ERM (chapter 2.4), the answers to specific questions were graded with the following scale:

- -2: Contradiction to proper ERM implementation
- -1: Possible contradiction to proper ERM implementation
- 0: Unsure of effect to proper ERM implementation
- 1: Probable indicates proper ERM implementation
- 2: Indicates ERM proper implementation

Some modifications had to be made to certain answers in order to apply the above grades. The results of questions 11 and 12 were calculated as percentages for each company, of the number of processes that answered Yes" comparing to the "No", excluding the "Does not exist" option. Also, from question 20 regarding the business tools, only the 3 were included (Risk matrixes, Formalized Management Review and Employee Feedback) as they can be considered essential to all companies.

The grades were given to each answer according to the Table 9.

Table 9 Grading matrix for maturity estimation

Question	**Grade -2**	**Grade -1**	**Grade 0**	**Grade 1**	**Grade 2**
6.Does the organization follow any specific framework Enterprise Risk Management?	Safety officer	I do not know	No	Special Consultant & Customer Trade Credit Insurance	BRC CAS ERM COSO ERM COSO ERM ISO 31000
7.Is there a dedicated role in the organization's chart relate to the ERM?		I do not know	No	Someone else	Yes
10.At what percentage of the annual turnover the organization applies ERM?	Up to 19%	20% - 39%	40% - 59%	60% - 79%	80% - 100%
11.In which of the organization's processes is the ERM applied?	Up to 19%	20% - 39%	40% - 59%	60% - 79%	80% - 100%
12.In which of the organization's processes are there specific and quantified objectives and tracking?	Up to 19%	20% - 39%	40% - 59%	60% - 79%	80% - 100%
13.If a new member arrives, how quickly and easily will he ascertain that in the organization Structures and roles related to ERM are established.	Disagree	Probably disagree	Neither agree nor disagree	Probably agree	Agree
13.If a new member arrives, how quickly and easily will he ascertain that in the	Disagree	Probably disagree	Neither agree nor disagree	Probably agree	Agree

Question	Grade -2	Grade -1	Grade 0	Grade 1	Grade 2
organization procedures for identifications and recording of risks are established.					
13.If a new member arrives, how quickly and easily will he ascertain that in the organization procedures for evaluating the severity of the risks established.	Disagree	Probably disagree	Neither agree nor disagree	Probably agree	Agree
13.If a new member arrives, how quickly and easily will he ascertain that in the organization procedures for prioritization of risks are established *Procedures for prioritization of risks*	Disagree	Probably disagree	Neither agree nor disagree	Probably agree	Agree
13.If a new member arrives, how quickly and easily will he ascertain that in the organization procedures of recording previously identified risks are established.	Disagree	Probably disagree	Neither agree nor disagree	Probably agree	Agree
13.If a new member arrives, how quickly and easily will he ascertain that in the organization procedures for monitoring changes in the external and internal environment are established	Disagree	Probably disagree	Neither agree nor disagree	Probably agree	Agree
14.In what way does Top Management distribute resources for the ERM?		There is no specific distribution	According to the situation	It is a part of each process's planning & It is a part of the annual plan	Formally, with a higher frequency than once per year
15.How frequently does Top Management include	Never	Rarely	Sometimes – When needed	Often	Always

Question	Grade -2	Grade -1	Grade 0	Grade 1	Grade 2
the results of ERM in the decision-making process?					
16.How often does Top Management sets specific actions for identified risks?	Never	Rarely	Sometimes – When needed	Often	Always
17.How often does Top Management review the outcomes of the actions taken for specific risks?			When needed	At least every 3 months At least every 6 months & At least every year	Every month
18.How often does Top Management review the performance of ERM?			When needed	At least every 3 months & At least every 6 months & At least every year	Every month
19.Is there a dedicated procedure regarding the ERM reporting to the Top Management?		No		Yes	
20.Fill in your affiliation with the presented business tools (Risk matrix)		I am aware of it, but it is not used & I have heard of it		It is used frequently & It has been used in the past	
20.Fill in your affiliation with the presented business tools (Formalized management review)		I am aware of it, but it is not used & I have heard of it		It is used frequently & It has been used in the past	
20.Fill in your affiliation with the presented business tools (Systemic feedback for the employees)		I am aware of it, but it is not used & I have heard of it		It is used frequently & It has been used in the past	

Having applied the above method of grading, the final result for each company came from the average of the individual questions. Using the scale from the Capability Maturity Model each company was categorized accordingly:

- <0 Initial - Ad hoc: The ERM process at this level of maturity is probably undocumented and in a state of dynamic change, tending to be driven in an ad hoc, uncontrolled, and reactive manner by users or events.
- <0.5 Repeatable – disciplined process: The ERM process at this level of maturity probably has some practices that are repeatable. The discipline is unlikely to be rigorous, but where it exists it may help to ensure that existing processes are maintained during times of stress.
- <1 Defined – standard: The ERM process at this level is defined and established. The process may not have been systematically or repeatedly used - sufficient for the users to become competent or the process to be validated in a range of situations.
- <1.5 Capable: The ERM process at this level probably effectively achieves the company's objectives and can be evidenced across a range of operational conditions. Process users probably have experienced the process in multiple and varied risks and are able to demonstrate competence.
- <=2 Efficient: At this level probably of maturity, the risk management principles are integrated fully within the management system and the focus is placed on the continuous improvement of the process.

As shown in figure 27, 72% of the surveyed companies are at the lowest two maturity levels, whereas the highest two consist of the 8%.

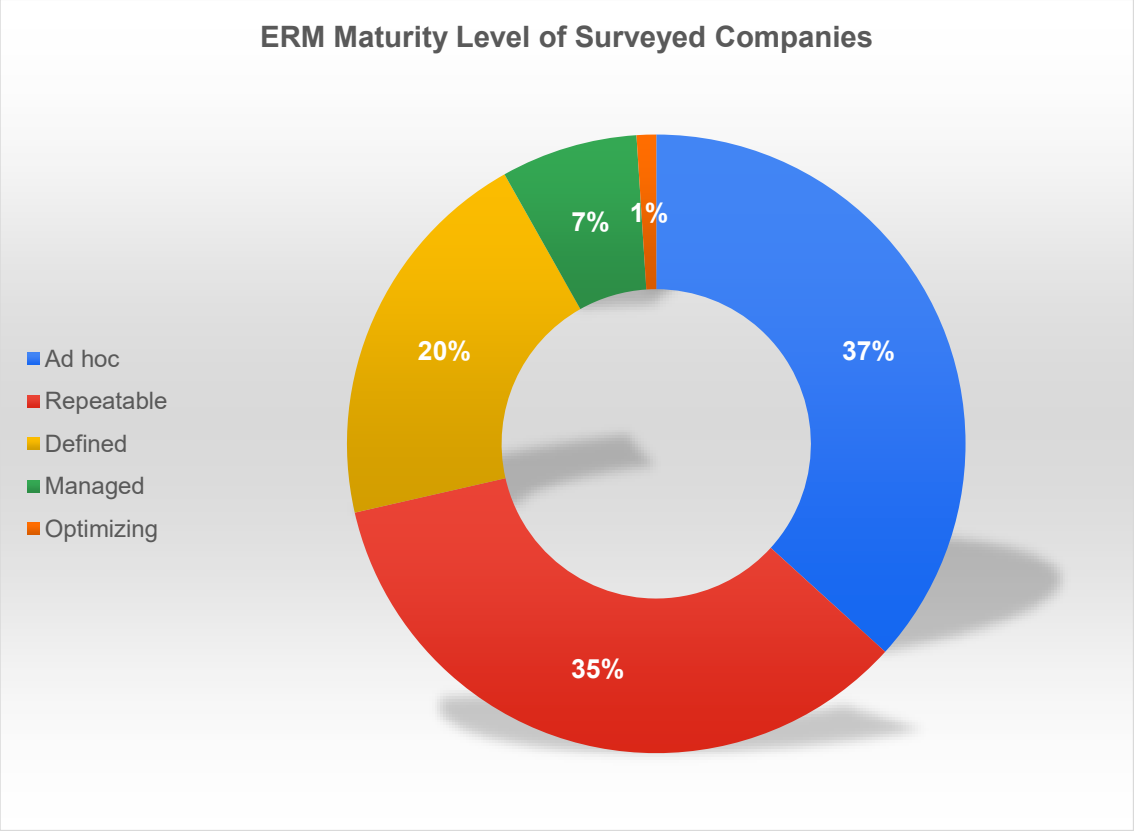
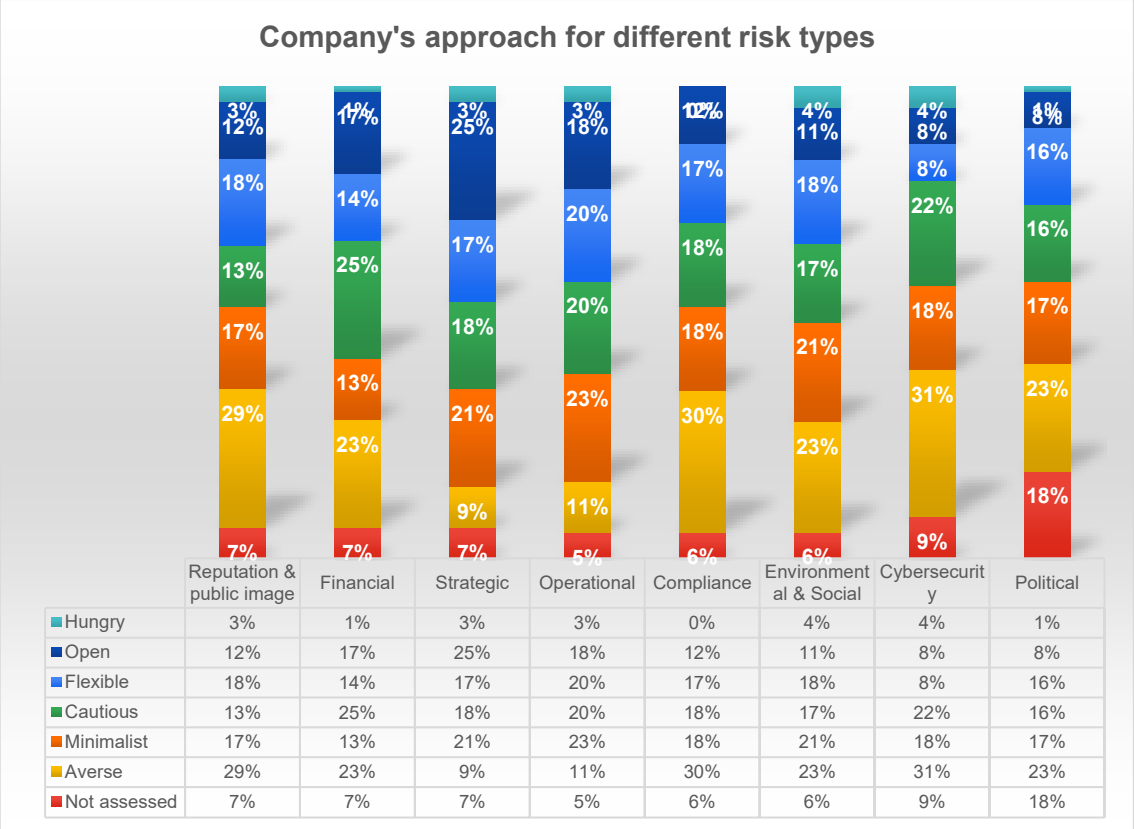


Figure 27 ERM Maturity Level of Surveyed Companies

5.2.2. What is the approach of Greek Companies regarding different risks?

The next question that is attempted to be answered by the survey is whether Greek companies have assessed all major risk types and how do the approach them.

By just switching the rows with the columns of figure 28 and looking at the answers in percentages, we can see that regarding reputation & public image (29%), compliance (30%), environmental & social (23%), cybersecurity (31%) and political (23%) risks the most prevalent approach was “Averse”. Similarly, for financial risks most common choice was “Cautious” (25%), for strategic “Open” (25%) and for operational “Minimalist” (23%). Compared to the others, political related risks received the highest percentage in the “Not assessed category” (18%).



	Reputation & public image	Financial	Strategic	Operational	Compliance	Environmental & Social	Cybersecurity	Political
Hungry	3%	1%	3%	3%	0%	4%	4%	1%
Open	12%	17%	25%	18%	12%	11%	8%	8%
Flexible	18%	14%	17%	20%	17%	18%	8%	16%
Cautious	13%	25%	18%	20%	18%	17%	22%	16%
Minimalist	17%	13%	21%	23%	18%	21%	18%	17%
Averse	29%	23%	9%	11%	30%	23%	31%	23%
Not assessed	7%	7%	7%	5%	6%	6%	9%	18%

Figure 28 Company's approach for different risk types

In order to identify the most common approach for each company, the Author counted how many times each approach was selected in the same company when it came to specific risks. In case of a tie the result was selected based on how the skewness of the distribution and if this was not possible, by comparing with the answers to question 10). “Averse” approach was the most frequent (26%), followed by “Minimalist” (24%), “Cautious” (21%), “Flexible” (17%), “Open” (10%), and the least selected was “Hungry” (2%).

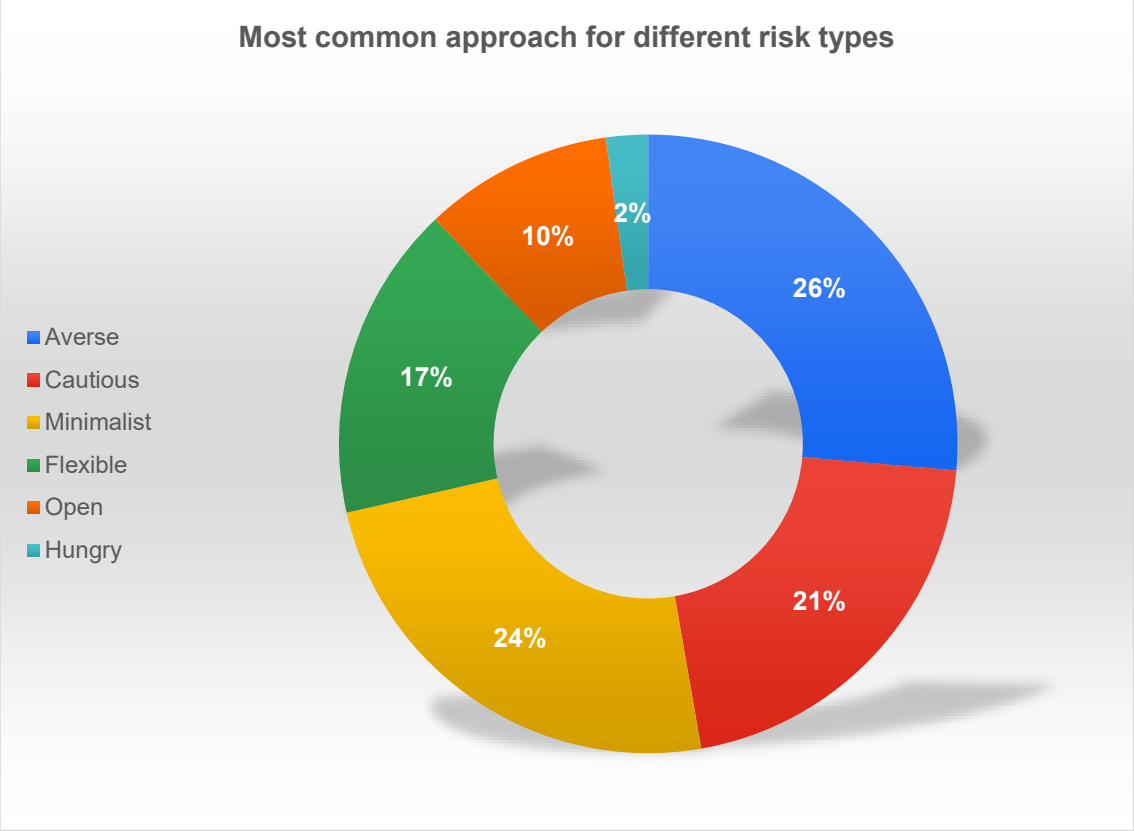


Figure 29 Most common approach for different risk types

5.2.3. How familiar are Greek companies with different business tools related to ERM?

The third point focused on this analysis is the use of business tools related to the ERM in Greece. By grouping the possible answers to the question 20 (Affiliation with the business tools) in to 2 categories, the ones that are or have been used in the company and the ones that have never been used we can see the familiarity of these tools. Unsurprisingly, the most commonly used tool is the “Cybersecurity software” at 82%, that can include a wide range of software, from a simple antivirus program installed in almost every computer to complicated and dedicated software for the prevention of cyber-attacks.

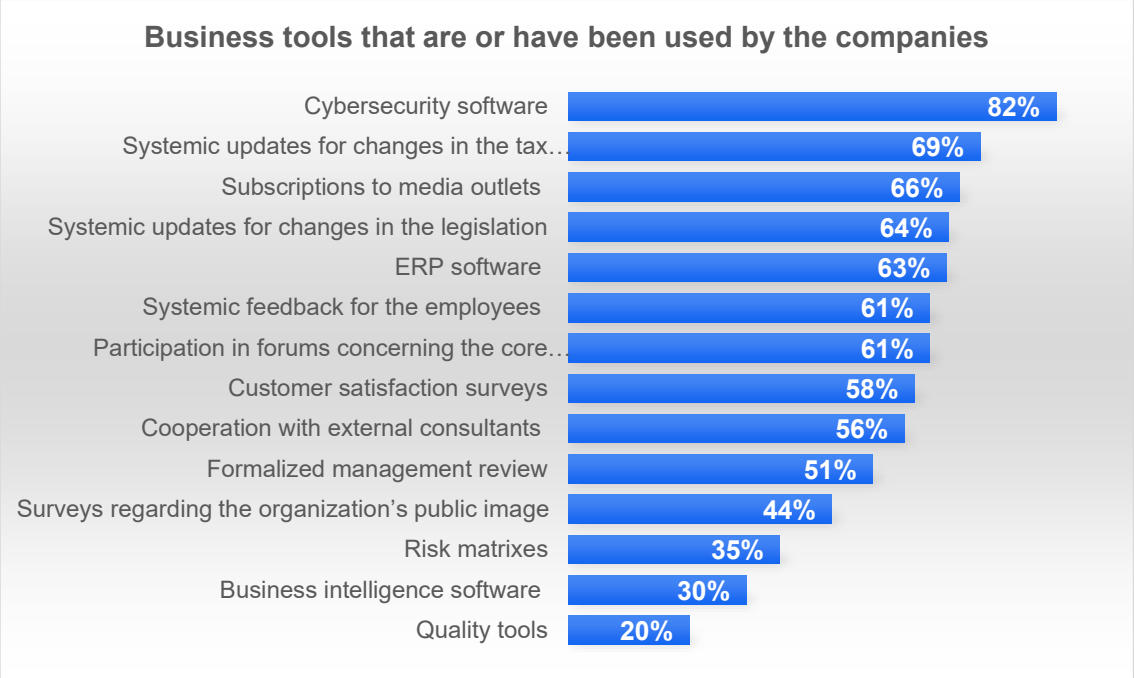


Figure 30 Business tools that are or have been used by the companies

5.3. Conclusion

Based on the results of the survey it appears that the concept of the Enterprise Risk Management is not largely integrated in Greek companies. With over one third of the surveyed companies reaching a grade lower than zero, it is evident that most companies do not approach risk management as a holistic idea, and some of them probably may not manage the risks in all aspects of their operation. The analysis shows that the ERM maturity level in Greece is low with most companies taking a reactive role in risk management rather than a proactive one, and the authors believes it is safe to assume that many companies still perceive risks only in a negative connotation.

By comparing the maturity level of the companies that are certified with at least one of the most common ISO standards, 9001, 14001 or 45001 (OHSA 18001 equivalent), we can observe a big difference in the results. 92% of the not certified companies are in the "Ad hoc" and "Repeatable" maturity levels, whereas for the certified ones these two levels amount to 60% (Figure 31). Still, even for the certified companies the maturity levels are low but based on the risk and opportunity culture these standards cultivate, substantial improvement can be noticed.

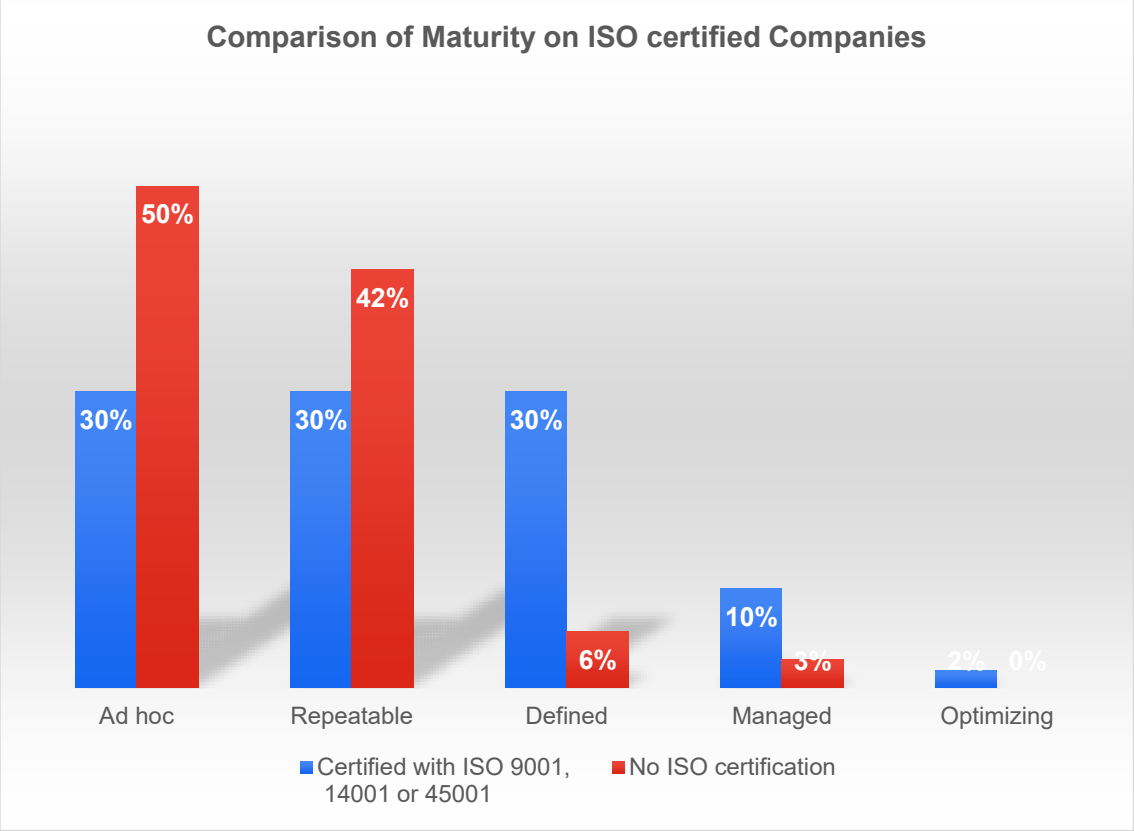


Figure 31 Comparison of Maturity on ISO certified Companies

This survey also tried to investigate the risk appetite of the participating companies. Even though most companies answered (figure 12) that they mostly take an open approach (Willing to consider all potential delivery options and choose the one that is most likely to result in successful delivery while also providing an acceptable level of reward), when contrasting the distributions with the most common answers to question 8 (figure 32) big discrepancies can be observed. When it comes to individual risks, companies selected more reserved answers with the prevalent being “Averse” (Avoidance of risk and uncertainty is a key Organizational objective). One possible explanation for this discrepancy is that maybe there is not a clearly defined risk appetite which can even cloud the vision of the responders of the questionnaire. Another explanation is that not all risk types receive the same focus, so in the estimation of the overall approach they are not considered equally. The only types of risk in which the most popular answer was not “Averse” were the financial (Cautious), the strategic (Open), and the operational (Minimalist). These risk types can be considered as more “traditional”, so more consideration could have been placed on them. If the rest types have not been evaluated sufficiently, it is logical to select the most reserved approach.

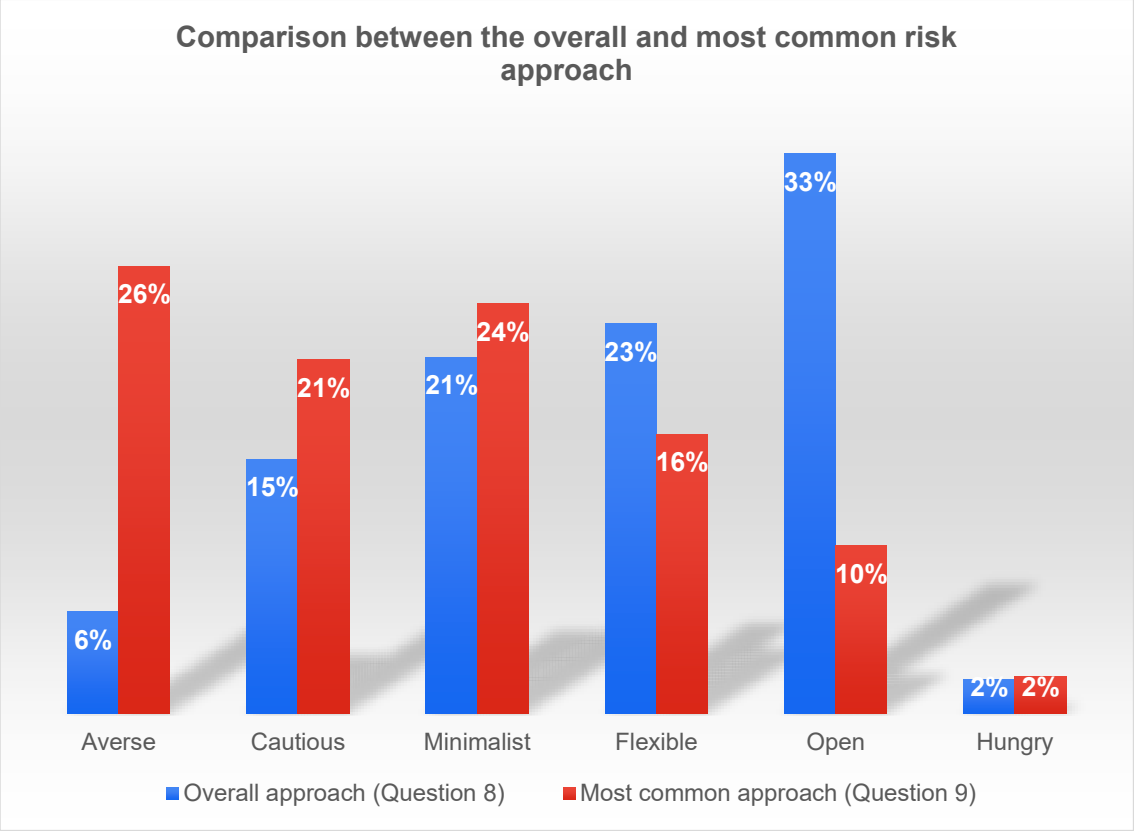


Figure 32 Comparison between the overall and most common risk approach

Finally, regarding the use of business tools, it is troubling to see low percentages in instruments that can greatly benefit any company. It is surprisingly to see such a low percentage in the usage of risk matrixes, since they are considered the most basic tool of risk assessment and are used by most companies, at least for the occupational health and safety risk assessment. The reasoning behind this percentage could be that even though risk matrixes exist in the company, they are not updated or used frequently. A formalized management review, that is only done approximately done by half of the surveyed companies, is an almost essential practice to assess the performance, define the strategy and plan all necessary actions. Regardless of the context of each company, some form of management review should take place, frequently, in all companies. Quality tools showed the least familiarity which can be expected, because they require a specific knowhow to apply them properly and many of them cannot be considered as transversal.

5.4. Limitations of the study

This survey aims to provide contribution to the theoretical approach as well as give an overview of the existing status however, each research design is associated with certain limitations. The limitations of this research are acknowledged and discussed as follows.

One difficulty that was identified early in the planning stage of the survey was the general inexperience with the relevant terminology in the Greek market. In order to assist the participants, the choice was made to form the questionnaire in Greek. Even so, based on the feedback, it appeared that some participants were not familiarized with the terminology and some questions might not have been understood fully. Furthermore, some hesitance was observed from a few participants in providing answers for their company since the topic relates to operational organizations, strategic views, and decisions (even though it was anonymous).

From a total of over 6500 emails sent, the survey was made base on the 98 receive answers. Even though there is a variety in the in the participants on the field of business, turnover, years in operation, etc. the results cannot be considered as a statistically accurate depictions of the current state of Greek companies. The survey presents an overview of the ERM application in Greece according to the participant's answers. Another limitation is the dependence on the answers provided questionnaire since there is no way to validate any of them. To acquire a precise view of the current status, specific audits or interviews must be conducted in companies representing all segments of the market.

The maturity estimation method was based on accredited literature but was developed specifically for the purpose of this master thesis, so the conclusions should be received as estimations. As a result, depending on the interpretation of the data collected, the outcomes of the evaluation can receive further examination and explanation.

.

5.5. Recommendations

In the previous concluding chapters the achievement of the objective of this master thesis is demonstrated. In this chapter the author gives his recommendations on how to improve the ERM diffusion and maturity level in Greece.

It is evident that although a lot of progress has been made globally in the adoption of proven busines practices, many companies still lack some fundamentals. Depending on the organization level and context of the company, it could prove overwhelming to try to implement everything all at once. The key to improvement is to set specific goals and lay achievable landmarks. In the case of ERM implementation the adoption of some of the tools described previously such as a management review, can provide added value to any company. A crucial aspect is the establishment of appropriate input methods since this is the beginning of everything. Again, by starting small with feedback from the employees, searching for relative information to the conduction of focused surveys, all companies must be able to perceive changes, and therefore risks in their environment. Any extra information will also help in the more efficient management of the risks identified.

From general to more structured processes, any company can benefit greatly by studying and applying the instructions of already existing ERM frameworks. Depending on the needs and available means of any organization, nowadays it is easy to have access to frameworks such as ISO 31000, COSO 2017, or many other self-assessment frameworks. By following any of these guidelines a company can have a clear understanding of what needs to be done and where are the weak points of its existing organization.

As seen in figure 31, the certification of the 3 core ISO standards (Especially 9001) can be the starting point for an ERM system. By addressing the requirements of the standards, the ERM process can be integrated more smoothly in the company's organization, since many of the requirements are common.

At one level or another all companies manage their risks; the real question is how well they do it? Risk management in some forms can be found in every organization but the point of ERM is to transition from a silo approach to a more holistic in order to achieve greater value creation. Companies should try to see the "bigger picture" and have a focal point of all their risks to better manage them. Just to provide a parallel example, all departments of the company are involved directly or indirectly with money transactions and funding. Efficient management cannot be achieved if everyone worked on its needs individually, that is why in all companies it is handled by a specific person or department. The same goes for risk management; the assignment of a dedicated person or team for this task can improve drastically the overall performance.

Lastly, an idea worth considering is the increase of legal requirement from only an occupational health and safety risk assessment to a Business risk assessment /

management system. As done in other countries, this would force all companies to further enrich their overall risk management approach. If done correctly, it should increase the viability of the companies and therefore strengthen the Greek economy.

5.6. Proposals for further research

Avenues for much extensive research on the topic can be derived from the findings and limitations of this thesis. As a proposal for other researchers the author suggests focusing on a defined segment of the Greek market and conducting interviews with a sufficient sample size. By doing so the research becomes more focused and the results less general.

Other topics that could also be considered are the estimation of the added value created from the proper implementation of ERM (maybe in the form of case studies), the collection and analysis of existing implementation methods and practices, or the comparison of the results from Greek companies with other similar countries.

6. References

International Organization for Standardization. (2011). *Global ISO 31000 survey 2011*. Retrieved from http://www.iso31000survey.com/Global_Survey_ISO_31000_English.pdf

Ansell, J., & Wharton, F. (1992). *Risk: analysis, assessment, management.* West Sussex: John Wiley & Sons, Inc.

Banham, R. (2007, June 01). *Is ERM GRC? Or Vice Versa?* Retrieved from Treasury & Risk: https://www.treasuryandrisk.com/2007/06/01/is-erm-grc-or-vice-versa/

Barton, T., Shenkir, W., & Walker, P. (2002). *Making Enterprise Risk Management Pay Off: How Leading Companies Implement Risk Management.*

Boritz, E. (1990). *Approaches to dealing with risk and uncertainty.* CICA .

Buehler, K., Freeman, A., & Hulme, R. (2008). *The Risk Revolution – McKinsey Working Papers on Risk. .* McKinsey& Company.

Cambridge University. (1995). *Cambridge dictionary.*

Chapman, R. (2012). *imple Tools and Techniques for Enterprise Risk Management.*

COSO. (1992). *Internal Control – Integrated Framework.*

COSO. (2004). *Enterprise Risk Management – Integrated Framework.*

COSO. (2017). *Enterprise Risk Management Framework - Integrating Strategy and Performance.*

Frigo, M., & Anderson, R. (2011). What Is Strategic Risk Management? *Stratgic Management*.

HM Treasury. (2004). *The Orange Book: Management of Risk - Principles and Concepts.* London: English Crown.

HM Treasury. (2006). *Thinking about riks. Managing your risk appetite: A practitioner's guide.* London.

Hopkin, P. (2012). *Fundamentals of risk management: understanding, evaluating and implementing effective risk management.*

Hoyt , R., & Liebenberg, A. (2011, 04 11). The Value of Enterprise Risk Management. *The jurnal of Risk and Insurance*.

Institute of Risk Management. (2002). *A Risk Management Standard.* Institute of Risk Management.

International Organization for Standardization. (2009). *ISO Guide 73, Risk Management - Vocabulary.*

International Organization for Standardization. (2015). *Quality management systems — Requirements.*

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

Kaplan, S. (1997). The Words of Risk Analysis. *Risk Analysis*.

Levine, D. (2013). *The GPS Framework: A New Approach to Comprehensive Strategic Risk Management.* Enterprise Risk Management Symposium.

Lexico. (n.d.). Retrieved from Lexico, powered by OXFORD: https://www.lexico.com/en/definition/risk

Neil, A., & Louise, B. (2006). *Strategic Risk: It's all in your head.* University of Bath.

Oxfrd University. (1884). *Oxford English Dictionary.*

Pagach, D., & Warr, R. (2010). *The Effects of Enterprise Risk Management on Firm Performance.* North Carolina: North Carolina State University.

Paulk, M., Curtis, B., Chrissis, M., & Weber, C. (1993). Capability maturity model, version 1.1. *Institute of Electrical and Electronics Engineers* .

Power, M. (2004). *The Risk Management of Everything.*

Prewett , K., & Terry, A. (2018). COSO's Updated Enterprise Risk Management Framework—A Quest For Depth And Clarity. *The journal of Corporate Accounting & Finance* .

Pritchard, C. L. (2010). *Risk Management: Concepts and Guidance.*

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

Renn, O. (2008). *Risk Governance: Coping with Uncertainty in a Complex World.*

Rittenberg, L., & Martens, F. (2012). *Enterprise Risk Management - Understanding and Communicating Risk Appetite.* COSO.

Rodriguez, E., & Edwards, J. (2009). Applying knowledge management to enterprise risk management: Is there any value in using KM for ERM? *Journal of Risk Management in Financial Institutions*.

Rubino, M. (2018). A Comparison of the Main ERM Frameworks: How Limitations and Weaknesses can be Overcome Implementing IT Governance. *International Journal of Business and Management*.

Stroh, P. (2005). *Enterprise risk management at UnitedHealth Group.* Strategic Finance.

Wiliams, C. (2019, April 8). *ISO 31000 VS. COSO – Comparing And Contrasting The World's Leading Risk Management Standards*. Retrieved from ERM Insights.

7. Annexes

7.1. Survey

Survey for the diffusion of Enterprise Risk Management in Greek companies

Αξιότιμοι συμμετέχοντες,

Το παρόν ερωτηματολόγιο αποτελεί μέρος διπλωματικής εργασίας του μεταπτυχιακού προγράμματος σπουδών MBA TQM, του Πανεπιστημίου Πειραιώς, με τίτλο «Diffusion of Enterprise Risk Management in Greek companies».

Ο μέσος χρόνος συμπλήρωσης του ερωτηματολογίου υπολογίζεται στα 14 λεπτά.

Οι ερωτήσεις αφορούν καθαρά το πλαίσιο λειτουργίας της εκάστοτε επιχείρησης, ως εκ τούτου, δεν υπάρχουν σωστές και λάθος απαντήσεις. Οι απαντήσεις σας σε όλες τις ερωτήσεις είναι ανώνυμες και εμπιστευτικές, και θα χρησιμοποιηθούν μόνο ομαδοποιημένες για τους σκοπούς της έρευνας.

Σας ευχαριστώ εκ των προτέρων για τη συμμετοχή σας,

Νίκας Γεώργιος

Μεταπτυχιακός φοιτητής (Α.Μ.: ΜΔΕΟΠ1713)

Τηλέφωνο επικοινωνίας: +306942244085

Για περισσότερες πληροφορίες μπορείτε να απευθυνθείτε στον επιβλέποντα Αναπληρωτή Καθηγητή, Μάρκο Τσόγκα.

https://www.unipi.gr/unipi/el/mtsogas.html

1. Σε ποιον κλάδο δραστηριοποιείται η επιχείρησή σας;

2. Πόσα χρόνια είναι σε λειτουργία η επιχείρηση;
   - 0 - 1
   - 1 - 5
   - 5 - 10
   - 10 - 15
   - 15 - 20
   - Άνω των 20

3. Ποιος είναι ο συνολικός αριθμός υπάλληλων που απασχολεί η επιχείρηση;
   - 1 - 9
   - 10 - 24
   - 25 - 49
   - 50 - 99
   - 100 - 199
   - 200 – 500
   - Άνω των 500

4. Η επιχείρησή αποτελεί μέρος ενός μεγαλύτερου οργανισμού;

- Ναι
- Όχι

5. Είναι η επιχείρηση πιστοποιημένη σύμφωνα με κάποιο από τα παρακάτω πρότυπα;
   - Όχι
   - ISO 9001
   - ISO 14001
   - ISO 45001 / OHSA 18001

6. Ακολουθεί η επιχείρηση κάποιο συγκεκριμένο πλαίσιο (framework) για την διαχείριση επιχειρηματικού κινδύνου (ERM);
   - Όχι
   - ISO 31000
   - COSO ERM 2017
   - COSO ERM 2004
   - CAS ERM
   - Άλλο…

7. Υπάρχει συγκεκριμένη θέση στο οργανόγραμμα της εταιρίας σχετική με το ERM; Εάν δεν υπάρχει αλλά το αναλαμβάνει αποκλειστικά κάποιος άλλος, παρακαλώ συμπληρώστε την θέση που έχει στο πεδίο "Άλλο".
   - Ναι
   - Όχι
   - Άλλο…

8. Ποια από τις παρακάτω εκφράσεις πιστεύετε ότι περιγράφει καλύτερα την προσέγγιση της εταιρίας για την διαχείριση ρίσκων;
   - Averse: Η αποφυγή ρίσκων και αβέβαιων καταστάσεων είναι βασικός στόχος.
   - Minimalist: Προτίμηση πολύ ασφαλών επιλογών οι οποίες έχουν πολύ μικρό βαθμό ρίσκου και ανταμοιβής.
   - Cautious: Προτίμηση ασφαλών επιλογών οι οποίες έχουν περιορισμένο βαθμό ρίσκου / ανταμοιβής.
   - Flexible: Προθυμία ανάληψης δικαιολογημένων ρίσκων, με τις ανάλογες ανταμοιβές.
   - Open: Προθυμία εξέτασης όλων των πιθανών επιλογών και επιλογή εκείνης η οποία είναι πιο πιθανό να επιφέρει τις βέλτιστες ανταμοιβές συνυπολογίζοντας ποιο είναι το αποδεκτό επίπεδο ρίσκου.
   - Hungry: προτίμηση καινοτόμων λύσεων οι οποίες μπορούν να φέρουν τις μέγιστες ανταμοιβές ανεξαρτήτως του επιπέδου του ρίσκου.

9. Δεδομένου ότι η κάθε επιχείρηση διαχειρίζεται με διαφορετικό τρόπο τις διακινδυνεύσεις ανάλογα με την φύση τους, παρακαλώ συμπληρώστε στον παρακάτω πίνακα την προσέγγιση της εταιρίας για κάθε έναν από τους παρακάτω τύπους ρίσκου βάσει των ερμηνειών της προηγούμενης ερώτησης:

	Not assessed	Averse	Minimalist	Cautious	Flexible	Open	Hungry
Reputation & public image							
Health and safety							
Financial							
Strategic							
Operational							
Compliance							
Environmental & Social							
Cybersecurity							
Political							

10. Σε τι ποσοστό του κύκλου εργασιών (ποσοστό πελατών) της επιχείρησης εφαρμόζεται το ERM;
    - Έως 19%
    - 20% - 39%
    - 40% - 59%
    - 60% - 79%
    - 80% - 100%

11. Σε ποιες από τις παρακάτω διεργασίες (processes) της επιχείρησης εφαρμόζεται το ERM:

	Ναι	Όχι	Δεν υπάρχει στην επιχείρηση η διεργασία
Accounting			
Customer Support / After Sales			
Finance			
Human Resources			
information technology (IT)			
Legal			
Management			
Marketing			
Product Development			
Quality and improvement			
Research and development			
Sales			
Supply chain			

12. Σε ποιες από τις παρακάτω διεργασίες (processes) υπάρχει συγκεκριμένη και ποσοτικοποιημένη θεσμοθέτηση στόχων:

	Ναι	Όχι	Δεν υπάρχει στην επιχείρηση η διεργασία
Accounting			
Customer Support / After Sales			
Finance			
Human Resources			
information technology (IT)			
Legal			
Management			
Marketing			
Product Development			
Quality and improvement			
Research and development			
Sales			
Supply chain			

13. Εάν έρθει ένα καινούριο στέλεχος στην επιχείρηση θα διαπιστώσει εύκολα και γρήγορα ότι στη επιχείρηση υπάρχουν:

	Διαφωνώ	Μάλλον διαφωνώ	Ούτε συμφωνώ ούτε διαφωνώ	Μάλλον συμφωνώ	Συμφωνώ
Δομές και ρόλοι σχετικοί με το ERM					
Διαδικασίες αναγνώρισης και καταγραφής διακινδυνεύσεων					
Διαδικασίες εκτίμησης της βαρύτητας των διακινδυνεύσεων					
Διαδικασίες κατάταξης προτεραιοτήτων των διακινδυνεύσεων					
Διαδικασίες καταγραφής παλαιότερων διακινδυνεύσεων (risk portfolio)					
Διαδικασίες παρακολούθησης αλλαγών στο εξωτερικό ή εσωτερικό περιβάλλον					

14. Κυρίως με ποιόν τρόπο η ανώτερη διοίκηση διανέμει πόρους (υλικούς και ανθρώπινους) για το ERM;
    - Δεν υπάρχει συγκεκριμένη κατανομή
    - Αναλόγως με την περίσταση
    - Συγκαταλέγεται στις ανάγκες της εκάστοτε διεργασίας
    - Αποτελεί μέρος του ετήσιου σχεδιασμού
    - Επίσημα, μεγαλύτερης συχνότητας της ετήσιας

15. Στα πλαίσια της επιχείρησης, η ανώτατη διοίκηση λαμβάνει τα αποτελέσματα της διαχείρισης του επιχειρησιακού κινδύνου στην λήψη αποφάσεων:
    - Σπανίως
    - Μερικές φορές – όταν χρειάζεται
    - Συχνά
    - Συνεχώς

16. Η ανώτατη διοίκηση εφαρμόζει ενέργειες διαχείρισης σε επιλεγμένες διακινδυνεύσεις:
    - Ποτέ
    - Σπανίως
    - Κατά περίπτωση
    - Συχνά
    - Συνεχώς

17. Η επιχείρηση κάνει αναθεώρηση των αποτελεσμάτων των ενεργειών που έχουν παρθεί για τις επιλεγμένες διακινδυνεύσεις:
    - Το αργότερο κάθε μήνα
    - Το αργότερο κάθε 3 μήνες
    - Το αργότερο κάθε 6 μήνες
    - Το αργότερο κάθε χρόνο
    - Κατά περίπτωση

18. Η επιχείρηση κάνει αναθεώρηση και ανασκόπηση των επιδόσεων του ERM:
    - Το αργότερο κάθε μήνα
    - Το αργότερο κάθε 3 μήνες
    - Το αργότερο κάθε 6 μήνες
    - Το αργότερο κάθε χρόνο
    - Κατά περίπτωση

19. Υπάρχει κάποια συγκεκριμένη διαδικασία αναφορών (reporting) προς την ανώτερη διοίκηση για το ERM;
    - Ναι
    - Όχι

20. Δεδομένης της μεγάλης ποικιλίας εργαλείων συλλογής, διατήρησης, ανάλυσης πληροφοριών και δεδομένων, είναι πολύ δύσκολο να έχει κάποιος προσωπική εμπειρία με όλα. Συμπληρώστε παρακαλώ την σχέση σας με τα παρακάτω εργαλεία:

	Τα έχω ακουστά	Το γνωρίζω, αλλά δεν το χρησιμοποιούμε στην επιχείρηση	Το έχουμε χρησιμοποιήσει στο παρελθόν	Το χρησιμοποιούμε συστηματικά
Πίνακες εκτίμησης κινδύνου (risk matrix)				
Έρευνες σχετικά με την δημόσια εικόνα της επιχείρησης				
Έρευνες μέτρησης ικανοποίησης πελατών				
Συστήματα ERP (SAP, Soft1 κ.α.)				
Προγράμματα Business Intelligence (Tableau, Power BI κ.α.)				
Συνδρομές σε έντυπα και άλλα μέσα ενημέρωσης				
Προγράμματα ψηφιακής ασφάλειας (Antivirus s/w, data encryption)				
Μέθοδοι ενημέρωσης για την νομοθεσία (συνεργασία με ΕΞΥΠΠ, συνδρομή σε έντυπα κ.α.)				
Δομημένη ανασκόπηση της Διοίκησης				
Εργαλεία ποιότητας (6 sigma, Pareto κ.α.)				
Μέθοδοι ενημέρωσης για τις αλλαγές στην φορολογία (Σεμινάρια , συνδρομή σε έντυπα κ.α.)				
Συμμετοχή σε forum ή ημερίδες σχετικές με τις βασικές λειτουργίες της επιχείρησης				
Δομές καταγραφής ανάδρασης (feedback) από				

τους εργαζόμενους				
Συστηματική συνεργασία με συμβούλους / συμβουλευτικές εταιρίες				

21. Πόσο ικανοποιημένος είστε με την διαχείριση της υγειονομικής κρίσης του COVID-19 από την επιχείρησή σας;
    - Καθόλου
    - 1
    - 2
    - 3
    - 4
    - 5
    - Πολύ

22. Έχει προχωρήσει η επιχείρηση σε ορισμό συγκεκριμένων ενεργειών για την διαχείριση των υπαρχόντων και μελλοντικών επιπτώσεων της κρίσης;
    - Ναι
    - Όχι

23. Ποιος είναι ο ρόλος σας στην επιχείρηση;

24. Ο ετήσιος κύκλος εργασιών της επιχείρησης για το 2019 ήταν:
    - Έως 999,999€
    - 1,000,000€ - 4,999,999€
    - 5,000,000€ - 9,999,999€
    - 10,000,000€ - 19,999,999€
    - 20,000,000€ - 39,999,999€
    - Άνω των 40,000,000€

25. Στο παρακάτω πλαίσιο μπορείτε να συμπληρώσετε ότι θα θέλατε να αναφέρετε για το ERM και δεν συμπεριλαμβάνεται στις παραπάνω ερωτήσεις:

Σας ευχαριστώ πολύ για τον χρόνο σας.

Εάν ενδιαφέρεστε να λάβετε τα αποτελέσματα της έρευνας, παρακαλώ συμπληρώστε στα παρακάτω πεδία τα στοιχεία επικοινωνίας σας.

Ονοματεπώνυμο
Email

7.2. Cover Letter

Subject: Μελέτη για την Διαχείριση Επιχειρηματικού Κινδύνου (Enterprise Risk Management)

Προς τον Διευθύνοντα Σύμβουλο, τα μέλη της Ανώτατης Διοίκησης ή τον Υπεύθυνο για την διαχείριση επιχειρηματικού κινδύνου

Αξιότιμοι συμμετέχοντες,

Ονομάζομαι Νίκας Γεώργιος και σας αποστέλλω αυτό το ερωτηματολόγιο στα πλαίσια της διπλωματικής μου εργασίας του μεταπτυχιακού προγράμματος σπουδών MBA Total Quality Management, του Πανεπιστημίου Πειραιώς, με τίτλο «Diffusion of Enterprise Risk Management in Greek companies». Η μελέτη προσπαθεί να κατανοήσει το επίπεδο της εφαρμογής της διαχείρισης επιχειρηματικού κινδύνου (Enterprise Risk Management) στην Ελλάδα, καθώς και τις μεθόδους και τα εργαλεία που χρησιμοποιούν οι ελληνικές επιχειρήσεις. Πρόκειται για μια από τις πρώτες μελέτες που γίνονται στην χώρα μας σχετικά με αυτό το θέμα, το οποίο προσελκύει αυξανόμενο ενδιαφέρον διεθνώς. Θεωρούμε ότι η σωστή διαχείριση των ρίσκων ενός οργανισμού είναι αναγκαία για να βελτιστοποιηθεί η απόδοσή του, κάτι το οποίο αποκτά ιδιαίτερη βαρύτητα εάν αναλογιστούμε τις επιπτώσεις που είχε σχεδόν σε όλες της επιχειρήσεις ένας καινούριος κίνδυνος, αυτός του COVID-19.

Στο τέλος του ερωτηματολογίου, συμπληρώνοντας τα στοιχεία σας (Email και όνομα) έχετε την επιλογή να λάβετε τα αποτελέσματα της μελέτης όταν εκπονηθεί. Οι ερωτήσεις αφορούν καθαρά το πλαίσιο λειτουργίας της εκάστοτε επιχείρησης, ως εκ τούτου, δεν υπάρχουν σωστές και λάθος απαντήσεις. Οι απαντήσεις σας σε όλες τις ερωτήσεις είναι ανώνυμες και εμπιστευτικές, και θα χρησιμοποιηθούν μόνο ομαδοποιημένες για τους σκοπούς της μελέτης.

Σας ευχαριστώ εκ των προτέρων για τη συμμετοχή σας,

Νίκας Γεώργιος

Μεταπτυχιακός φοιτητής (Α.Μ.: ΜΔΕΟΠ1713)

Τηλέφωνο επικοινωνίας: +306942244085

Για περισσότερες πληροφορίες μπορείτε να απευθυνθείτε και στον Επιβλέπων Αναπληρωτή Καθηγητή, Κ. Μάρκο Τσόγκα.