Department of Business & Management – Chair in Risk Management

Enterprise Risk Management, Internal Audit, and the other control functions in Italian listed companies.

Supervisor
Prof. Vittorio Vecchione

Candidate
Valeria De Luca
668481

Co-supervisor
Prof. Cristiano Cannarsa

Academic Year 2015/2016

Index

Executive summary

During the last decades, the attention that regulators, entities and stakeholders addressed to risk management changed drastically because of the occurrence of specific events, as financial crises and natural catastrophic events, and because of a new diffuse perception about risk. Indeed, while risk was considered before only as a negative element and the potential positive effects of the upside volatility were not accounted, nowadays entities understand that a risk might represent a resource and an opportunity if well managed. Therefore, even the way in which risks are managed had to change to reflect this different risk perception.

Traditional risk management systems were mainly dependent on a historical-data treatment of risk and mainly focused on financial risks (failing to consider the wide range of risk types). Moreover, they were mainly based on a silos-approach in managing risks, and they were not conducting a risk-return analysis able to support decision-making and to ensure the maximization of shareholders' value. Nowadays, the best practice in risk management is Enterprise Risk Management (ERM). This practice is defined by COSO (2004) as "a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives". Therefore, as emerge by the definition above, this best practice seems to overcome the typical issues of the traditional systems.

There is a wide set of guidelines, principles and standards about ERM, and, because of it, it might be believed that this practice is widely implemented by entities.

The first chapter of this thesis presents a study on ERM conducted to assess, over a sample of 30 Italian listed companies, if this best practice is actually diffuse or if it remains only a theoretical suggestion.

After presenting all the possible methodologies to conduct the analysis, it is described the one chosen. Gathering information directly from the entity through a careful analysis of the Corporate Governance Reports has been considered as the best way to obtain trustful information and to reduce the subjectivity that could otherwise be faced when letting employees discuss and score their risk management system. However, because of this methodology, it has to be kept in mind

while reading this thesis that any evaluation has been made on the base of what entities declared in their official documents.

Each of the three studies conducted in this thesis has used as sample of companies a heterogeneous group of 30 Italian listed companies having different sizes (in terms of market capitalization) and exercising their activities in different sectors.

To assess the level of implementation of ERM, a group of key elements of enterprise risk management has been identified in line with COSO's definition, and a set of scores has been assigned to each of these elements. Whereupon, it has been assessed if and in which measure these elements were declared by entities in their CGRs.

Therefore, with the information obtained from the analysis conducted, it has been built a table (table 1.2) containing the partial scores and the sum of the partial scores gathered by each company.

The main conclusions obtained by the first study of this thesis are:

- Entities seem to understand the relevance of a well implemented ERM, but the majority of them appears more focused on formally comply with the directives rather than on making efforts to actually implement a good risk management system. A formal compliance let arise doubts on the goodness for the entities' statements implementation. It appears indeed dubious that these organizations, even being different and having different governance structures, report exactly the same aspects when describing the SCIGR.
- Some specific aspects of the entities influenced their ranking. Indeed, it resulted that bigger companies, because of their greater complexity and need to ensure protection against risk and because of their biggest amount of resources available, implement more mature risk management systems. Other aspects that emerged to influence the result of the research have been the sector in which the entity operates and the geographic scope that the entity has.

After that the ERM has been described and that its implementation within the sample of Italian listed entities has been assessed, it is introduced in chapter 2 the theme of risk governance. This latter represents the architecture within which risk management operates" (Corporate

Governance Council, 2012). Identifying how roles and responsibilities within ERM are settled, divided and assigned to people part of the organization, risk governance ensures a suitable level of control on the implementation and execution of the activities needed to manage risk.

Even if it is not possible to generalize because every entity might adopt a different risk governance, there are some roles and responsibilities that every entity should have. Chapter 2 shows some of the main actors involved in risk governance (BoD, "Comitato Controllo e Rischi",Director of the SCIGR, CRO) and their responsibilities.

Moreover, when presenting the internal audit function and the risk management function, it goes more in detail describing the Three Lines of Defense Model. This latter involves the participation of three groups of actors, each one of them resulting fundamental for the good result of the risk management system. Risk owners (1st line) are the ones better knowing the business and the issues arising from it. They are the most appropriate to identify risks, assess them, mitigate them and then monitor them. Risk managers (2nd line) are needed to ensure coordination among the actions undertaken by the different risk owners. Their intervention is fundamental to train and guide risk owners in the execution of their duties and to let them contribute to the respect of the risk limits attributed to the function and of the general risk appetite set for the organization. Finally, internal auditors (3rd line) are fundamental to ensure that the system receives independent and objective assessments to guarantee that the control and risk management system is implemented properly and that the strategic objectives are met.

The Model gives an easy and effective method to increase communication on risk management and control through the definition of specific roles and responsibilities. When the lines of defense are properly implemented, it should be reduced the possibility of gaps in control and of duplication actions, and there should be a greater probability to proper address and manage risk and control.

The role that internal audit has in risk management is furtherly analyzed in the 3rd chapter. Indeed, after an initial explanation of the necessity to ensure independence and objectivity to the internal audit function, it is presented the "fan of roles" that IA should undertake/undertake with safeguards/or not undertake. This fan, contained in a Position Paper of the IIA (2004), shows in the left side the assurance roles (core roles of the IA), in the center the consulting services roles (to be undertaken only with safeguards) and in the right side those roles that are normally played by the risk management function. From this fan and from the Three Lines of Defense Model, it is clear the

necessity of both these function in managing risks, as well as the necessity to clearly define roles and responsibilities of each function so that overlaps or gaps are avoided.

Once that the theoretical elements on which base the 2nd study of this thesis have been given, in this chapter are assessed the roles that the IA function of the 30 Italian listed companies actually plays in terms of risk management. This research has been based as well on the Corporate Governance Reports. For every entity it was looked in the report for the declaration produced by each organization in relation to the audit activities conducted during 2015 and in relation to responsibilities that this function generally has. Furthermore, on the base of these information, reported in table 3.1, it has been assessed which kind of roles the IA function of these entities is actually undertaking.

The main conclusions obtained from the second study of this thesis are:

- Almost all entities appear to formally comply with what required by the Codice di Autodisciplina for the internal audit (7.C.5). This formal compliance not only let appear the entities' declarations ambiguous, but it let all roles assumed by this function result as "assurance". Indeed, the Criteria 7.C.5 identifies mainly an assurance role for this function.
- Only one company of the sample (Parmalat) has the IA function that undertakes roles that should be attributed to the risk management function. Instead, the 50% of these entities declare that their IA functions not only provide assurance, but also consulting services.
- Only the 20% of these entities resulted to enlarge the description provided appearing not only to formally comply. Furthermore, it has been assessed that elements as the size and the sector in which the entity operates have influenced this result.

As emerged in what described above, the subjects involved in risk governance are numerous and each one responds and is accountable for the responsibilities to him attributed. Their expertise and their contribution are fundamental for the good output of the system. However, what results more fundamental is to ensure that coordination and communication mechanisms are in place to allow these subjects to share information and dispose of all the data needed to exercise their activities and facilitate the organization in exploiting the opportunities arising and reaching the objectives set in the strategic plan.

The concept of ensuring an efficient and effective risk management and control system where overlaps and gaps are avoided has assumed great relevance in the last years. Moreover, starting from this year, the Codice di Autodisciplina has requested companies to explicitly declare the coordination methods implemented.

This thesis investigated also how entities are actually coping with this new requirement and how much relevance they give to the coordination between the actors involved. As done with the other studies, before to start the research, a wide description is provided about the principles, standards and guidelines about coordination available to entities.

This 3rd and last research investigated the coordination mechanisms implemented by the sample of the 30 Italian listed companies. This study has been conducted on the base of what these organizations reported in their CGRs in the dedicated paragraph (required starting from this year by the Code).

The main conclusions obtained by the 3rd study of this thesis are:

- 70% of the entities part of the sample are explicitly declaring the coordination mechanisms implemented between all the actors involved. However, it appears that, even in this case, companies have mainly formally complied with what required. It emerges then that, even if organizations are trying to implement the new requirement, they still have to make many efforts to actually do it;
- The coordination methods that mostly recurred in the CGR are “the clear definition of roles and responsibilities” and “information flows and institutional meetings/reporting”;
- Financial entities seem to better implement coordination mechanisms.

1. ERM - research on its level of implementation within Italian entities

1.1 Risk

Risk management is an increasingly important process within a company and is considered one of the main drivers for a business. Thus, while companies are starting to implement advanced risk management systems, stakeholders are becoming constantly more concerned about and focused on risk.

Historically, a negative connotation has always been attributed to risk, associating it with the possibility that an adverse event would occur. In the everyday life, the possibility to get injured, to lose the job, or to suffer a theft have always been considered among the main risks that a person could face. Also in the economic environment, companies tried to contain the negative deviations from expected results, as the possibility to lose market share or to make a wrong investment, without paying attention to the positive aspects and consequences that could be brought by risks.

Nowadays, instead, companies are more aware of the importance that risk has and of the impossibility to completely eliminate it.
The definition of risk is “any deviation from expected”, meaning that the outcome obtained is different from the one planned. According to this definition, then, it is extremely important to consider the “downside volatility” as well as the “upside volatility” that may arise. Therefore, in order to increase the value of the firm, companies conduct risk-return analysis over the risks they are facing, and decide which risks should be avoided and which, instead, should be undertaken (Segal, 2011).

For these reasons, risk appears as a driver of strategic decisions and, if well managed, it may let companies develop a competitive advantage over the others. Therefore, the role of risk management is continuously growing and companies are developing and implementing better systems and processes to be able to exploit the opportunities and overcome the challenges related to the risks they are facing.

Due to environmental changes, to company's awareness of risk relevance, and to specific events, risk management evolved among decades.

1.2 Evolution of risk management

During the history, companies and their employees have always dealt with risk, but the way in which they used to do it changed over the time, improving and adapting to meet the new internal and external needs.

According to Crouhy, Galai, Mark (2014), the risk management system was initially extremely dependent on a historical-statistical data treatment of risk. Therefore, it was based on the assumption that past events would have occurred again in the future, failing to consider the possibility that a new unexpected scenario could have emerged. In managing risks, companies were then adopting a passive approach based on past experiences.
Moreover, because of the inability to quantify strategic and operational risk, available data were related just to financial risk and companies were failing to include all risk categories.

According to Sekerci (2011), each risk was managed in isolation, rather than on an integrated base, among the different units and departments of the firm.
As stated in the article of Bugalla and Narvaez (2014), negative consequences of this so called "silos approach" resulted to be:

- Creation of miniature ecosystems, each adopting different practices to manage risks. Having each ecosystem a risk culture and philosophy misaligned with those of the others, internal inconsistence arose;
- Rising of inefficiencies, caused by the absence of communication and coordination among the different departments, mainly represented by duplication of risk-mitigation efforts;
- Lack of completeness, resulting in the inability to measure the impact of more risks occurring simultaneously (sometimes even offsetting each other).

All the problems above made it more difficult for a company to fully and properly understand and address the key risks faced. Indeed, while firms may operate in unrelated businesses, a risk is able to affect simultaneously all of them.

According to Segal (2011), traditional risk management systems were too much concerned just about downside risk and mitigation plans to reduce the exposure. The lack of a proper risk-return analysis was mining the success of these systems that were failing in considering upside volatilities and, therefore, in exploiting profit opportunities.
Moreover, lacking to provide an integrated view of risks and returns, traditional risk management failed to support management decision making.

Furthermore, traditional risk management systems failed to consider the aggregated picture, missing the enterprise-wide scope typical of the recent systems.

All these failures, which appeared to be already no longer sustainable by firms, have been stressed by the occurrence of particular events, as the financial crises and natural catastrophic events, and by the emergence of those so called “black swans” risks, like terrorism attacks. All these situations let firm develop awareness for worst-case scenarios, whose likelihood could be low but whose impact could have a huge disruptive power over the company. Furthermore, firms understood the importance of considering risks in an integrated and aggregated way and of including all types of risk in the assessment. A dynamic and global vision was, then, required (Segal, 2011).

Nowadays, Enterprise Risk Management (ERM) is considered as a best practice in managing risk.

1.3 Enterprise Risk Management (ERM)

According to the Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2004), ERM is defined as “a process, effected by an entity’s board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives”.
This definition embeds some fundamental concepts that make this new risk management system differ from the previous ones.

Indeed, COSO's statement identifies ERM as a "process", an ongoing, evolving and cyclical process that goes through risk identification, risk quantification, risk decision-making and risk messaging.
This management system is "effected by people at every level of an organization", meaning that it is no longer responsibility of small groups of empowered people to deal with the different events that are faced. A risk culture is developed within the company, and everyone comply, then, with a specific risk philosophy that allows the firm to manage risks in an integrated way.
ERM is applied in "strategy setting" and, through the use of risk-return assessments, it helps the company to take valuable decisions and exploit profit opportunities. The main strategy adopted by firms to deal with risk is no longer only the acquisition of hedging instruments, rather is an expert and aware assessment of all the possible deviations from expected with a consequent balance of profit opportunities to be exploited and risks to be hedged.
Enterprise risk management is "applied across the enterprise", at every level, unit and business, and involves taking an enterprise level view of risk. Aggregated metrics are used and the overall volatility of the company is considered and managed within the enterprise risk appetite.
This management system is "able to provide reasonable assurance" to the management and BoD of an entity. Experts take part to the process and assess, through the use of various methodologies including scenario analysis, the main risks and determinate the impact that they would have on the company value. Furthermore, once that the risk is quantified and strategic actions are undertaken to address it and assure the achievement of entity's objectives, the outcome is messaged to stakeholders.

As defined in the ISO 31000 (2009), risk management "is not a stand-alone activity that is separate from the main activities and processes of the organization. Risk management is part of the responsibilities of management and an integral part of all organizational processes, including strategic planning and all project and change management processes."
From this definition as well, it is possible to evince that risk management should no longer be a stand-alone process. Rather, it should be an integrated process that provides support to strategic planning and decision making.

According to the Casualty Actuarial Society, ERM is defined as "the discipline by which an organization in any industry assesses, controls, exploits, finances and monitors risk from all

sources for the purpose of increasing the organization's short- and long-term value to its stakeholders".

ERM is an extremely important tool to help companies to accomplish with their first objective, create value for stakeholders, by conducting risk-return assessments over the value of the entire enterprise.

Contrarily to traditional risk management systems, ERM adds to the analysis of past data a specific focus on “potential events” and includes all risk categories.

As can be observed by the above definitions, ample regulations and frameworks are available for an “improved” risk management. Among the majors, we can list the COSO Enterprise Risk Management Framework and the International Standards Organization’s ISO 31000:2009, *Risk management – Principles and Guidelines on Implementation*. Furthermore, nowadays, many Stock Exchange Commissions require listed companies to disclose the risk management function and impose them specific standard in order to ensure an independent risk committee and CRO. Moreover, the market is rewarding companies that have a well implemented risk management system, as can be observed by the attention that credit-rating agencies as Moody’s and Standard & Poor’s (S&P) are putting on evaluating firms on the base of how they manage risk.

With such a plenty of standards, principles and guidelines, we might think that risk management is a settled practice with unanimous proven concepts and tools that demand only regulation to be put in place.

The aim of the next paragraphs is to assess if the above consideration is valuable for the sample of firms that are hereby analyzed. Is ERM a best practice in risk management widely spread among companies or is it a best practice to enhance value for shareholders that still needs to be implemented?

1.4 Research to assess the current status of implementation of ERM

1.4.1 Research methods

There are different methodologies used in literature to measure the level of implementation of ERM within an entity. The purpose of this paragraph is to briefly present them and to explain why the one used in this research has been preferred over the others.

A first method to assess ERM is to gather information needed to make the assessment directly from the company. In order to do it, two main methodologies are identified.
A possible solution is to survey firms, as Beasley et al. (2005) did. The target interviewees are identified, the core area of interest is set and a list of question is prepared. Available options would be let interviewee freely answer the questions or let them score the level of ERM implementation within their company and then argument their valuations. The criticalities of those options are that interviewee, answering freely, might lose the focus of the research, and, scoring ERM, might produce inconsistent information. In any case, survey firms is a methodology extremely influenced by subjectivity and interviewee might let the risk management system implemented within their companies appear better than how it really is. Furthermore, to make surveys to firms and to wait for their responsiveness would extremely influence the speed of conducting the study.
The second solution is, instead, to look for the information needed in the official documents published by the company. Of great relevance is the Corporate Governance Report, where firms disclose important data related, i.e., to the risk management systems, the CRO and important committee. The main challenge of this method is that these published documents may provide limited and standardized information and attention is needed to identify the small differences emerging between the risk management systems of the various entities.

An easy method to assess the ERM system of many entities is to use ratings provided by S&P as a proxy for the level of implementation. Unfortunately, this methodology, that has been used i.e. by Baxter et al. (2010), cannot be leveraged for a wide range of entities. Indeed, S&P provide these ratings just for a limited type of organizations.

Many studies (as those of Pagach and Warr, 2008 and 2011) based the analysis on CRO hiring announcements. The criticality emerging from this approach is that, being the position of CRO popular and sometimes even required by authorities (as stock exchange authorities), companies might have formalized this position without having actually implemented an ERM system.
Furthermore, this aspect would be extremely marginal and incomplete to build a comprehensive analysis. Indeed, to have a CRO is not the only component needed to develop a good risk management system, and companies might have a good ERM empowering a person with the same responsibilities of a CRO, without actually having a CRO.

To conduct this study, I chose to directly take information from the company. This method, that appears to be more complete than the others, can be used to assess and include in the research all types of entities, overcoming limitations embedded in the S&P's rating method.
Between the two possibilities to gather data directly from the firm, I preferred to refer to the published documents rather than to make surveys. Even if this latter option might provide more detailed information, giving the possibility to go deeper on relevant aspects, I thought that the high level of subjectivity and the lack of certification of the answers would have undermined the result of my research. Furthermore, the use of surveys could have caused delays in the study in case of slow responsiveness.
Instead, when dealing with entity's documents, the risk to obtain false information and to incur in interviewees' subjectivity is reduced. In order to comply with the numerous regulations and to avoid legal measures against the firm, different levels of control are appointed to ensure that the data provided in official documents represent the truth.

1.4.2 Entities' sample

The sample of italian companies that are included and assessed in this research is composed by 30 listed firms. In order to make this sample group more heterogeneous as possible, I chose the entities paying attention to their size (in terms of market capitalization) and to the macrosector and the sector in which they operate. Information about these firms has been taken from the list of Italian listed companies published by Borsa D'Italia the 31th of May 2016.

The first criteria followed to narrow down the list is to take the first 15 firms in terms of market cap participating to the FTSE MIB basket and the first 15 participating to the FTSE ITALIA MID CAP basket. This criterion allowed including companies of different sizes. For the study, companies of the FTSE ITALIA SMALL CAP and of the FTSE ITALIA MICRO CAP baskets have not been considered. The rationale behind this decision has been the lack of quality in their reports and the really small dimension/relevance they have compared with the others.

Once these entities have been selected, a second check to assure heterogeneity has been conducted. The macrosector and the sector in which they act have been identified. This second criteria provided a certain level of confidence and no adjustments in the sample were needed.

In table 1.1 is presented the final sample of entities.

Table 1.1: *Entities' sample*

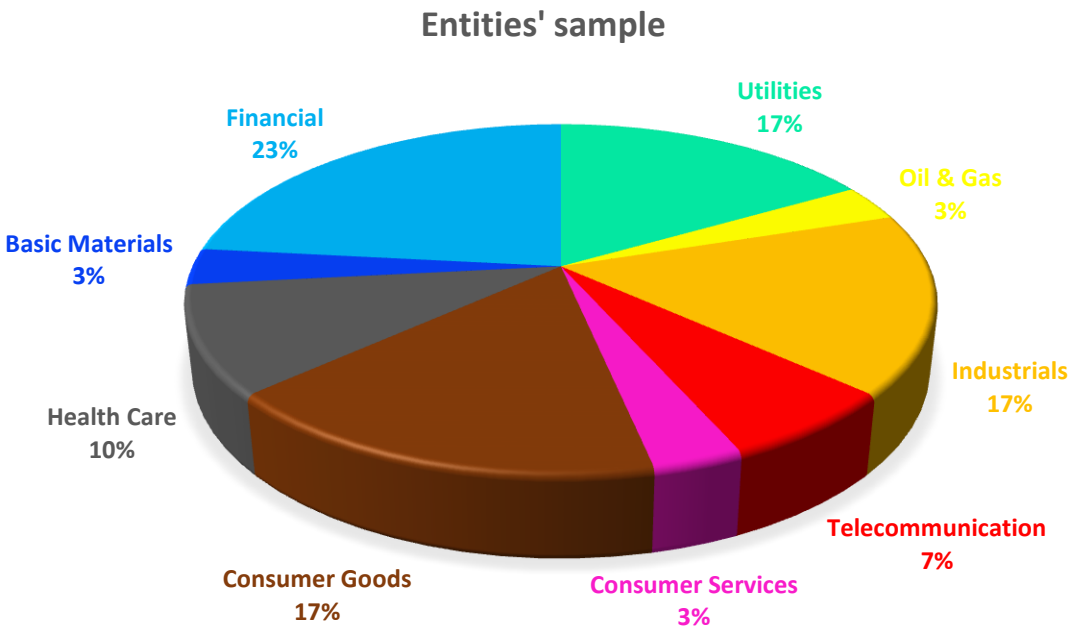
Entity	Market Cap		Basket	Macrosector	Sector
	(€ m)	(% tot)			
ENI	50293.79	9.93%	FTSE MIB	Oil & Gas	Oil & Gas
ENEL	41654.37	8.22%	FTSE MIB	Utilities	Utilities
Intesa San Paolo	36948.01	7.29%	FTSE MIB	Financials	Banks
Luxottica Group	23640.07	4.67%	FTSE MIB	Consumer goods	Personal & Household Goods
Generali	20515.75	4.05%	FTSE MIB	Financials	Insurance
Atlantia	19998.56	3.95%	FTSE MIB	Industrials	Industrial goods & Services
Unicredit	18036.54	3.56%	FTSE MIB	Financials	Banks
Snam	17995.06	3.55%	FTSE MIB	Utilities	Utilities
Tenaris	14114.57	2.79%	FTSE MIB	Basic Materials	Basic resources
Telecom Italia	11519.53	2.27%	FTSE MIB	Telecommunications	Telecommunications
Terna	10042.58	1.98%	FTSE MIB	Utilities	Utilities
Poste Italiane	8988.84	1.77%	FTSE MIB	Financials	Insurance
CNH Industrial	8660.96	1.71%	FTSE MIB	Industrials	Industrial goods & Services
Exor	8397.57	1.66%	FTSE MIB	Financials	Financial services
Fiat Chrysler Automobiles	8257.87	1.63%	FTSE MIB	Consumer goods	Automobiles & parts
Recordati	5539.08	1.10%	FTSE ITALIA MID CAP	Health Care	Health Care
Parmalat	4281.54	0.85%	FTSE ITALIA MID CAP	Consumer Goods	Food & Beverage
Hera	3919.88	0.78%	FTSE ITALIA MID CAP	Utilities	Utilities
De' Longhi	3609.95	0.72%	FTSE ITALIA MID	Consumer Goods	Personal &

			CAP		Households Goods
Brembo	3450.21	0.69%	FTSE ITALIA MID CAP	Consumer Goods	Automobiles & parts
Diasorin	3040.23	0.61%	FTSE ITALIA MID CAP	Health Care	Health Care
Acea	2812.52	0.56%	FTSE ITALIA MID CAP	Utilities	Utilities
Banca Generali	2758.34	0.55%	FTSE ITALIA MID CAP	Financials	Financial Services
Inwit	2587.84	0.52%	FTSE ITALIA MID CAP	Telecommunications	Telecommunications
Ima	2164.04	0.43%	FTSE ITALIA MID CAP	Industrials	Industrial Goods & Services
Credito Emiliano	1936.21	0.42%	FTSE ITALIA MID CAP	Financials	Banks
Ansaldo STS	2051.96	0.41%	FTSE ITALIA MID CAP	Industrials	Industrial Goods & Services
SIAS	2006.45	0.40%	FTSE ITALIA MID CAP	Industrials	Industrial Goods & Services
Amplifon	1987.49	0.40%	FTSE ITALIA MID CAP	Health Care	Health Care
Autogrill	1982.29	0.40%	FTSE ITALIA MID CAP	Consumer Services	Travel & Leisure

As can be observed in the table above, entities composing the sample can be grouped on the base of the macrosector in which they operate as follows: seven entities operate in Financial, five in Utilities, one in Oil & Gas, five in Industrials, five in Consumer Goods, one in Consumer Services, three in Health Care, two in Telecommunication, and one in Basic Materials.

Graph 1.1 shows this distribution.

Graph 1.1: *Entities distribution on a macrosector base.*



1.4.3 Guidelines to develop the research – Data gathering and process description

Once the sample has been identified, it is important to describe how this research has been handled out in order to assess whether or not Italian companies are implementing a good ERM system, and the level of maturity of this system.

As already explained, the information on which I base this study is directly taken by Corporate Governance reports. However, which are the data extrapolated from the official documents and how are they used within the research?

The first step in this research has been to identify some key elements within the reports. These aspects represent core factors to assess the risk management system of the thirty entities, and the presence or not of them in the official documents is an important indicator for the study. The definition of ERM provided by COSO and the characteristics of ERM identified in paragraph 1.3 have been fundamental in the choice of these elements.

The second step has been to define a range of grades for each factor previously defined. Indeed, according to what entities in the sample have reported in their official documents, the presence of

and the way in which key elements are described and implemented within the entity determinate the score, within the previously defined range, that each company awards for each key element.

The third step has been, then, to assess the presence of these elements in the description of the risk management system of each entity, as defined in the Corporate Governance Report, and to assign them a score.

Once that all entities and the key aspects have been analyzed, a further step has been to create a graduator of the companies on the base of the final total score they got (as sum of the partial scores for each different element) and to determinate the average score assigned for every key element.

Finally, the fifth step has been to evaluate the results obtained, both in terms of graduator of companies and of degree of implementation of every component, in order to create some final considerations on the level of implementation of ERM.

1.4.4 Research development

According to the first and second steps identified in paragraph 1.4.3, after having considered COSO's definition of ERM and, generally, the characteristics that this system should have, the key elements have been identified and a range of scores has been assigned to them.

Below, is presented the chosen list containing and describing these key factors and their relative scores:

ERM as a "process"

According to Segal's (2011) focus on ERM, risk management is an ongoing, evolving and cyclical process that goes through risk identification, risk quantification, risk decision-making and risk messaging. Therefore, for the aim of this study, it is important to assess if entities switched from a singular activity conducted to manage an emerged risk to a process having the scope to follow the risk from the identification until the messaging. Furthermore, this process should be continuous

and involve the monitoring of risks even after that actions to mitigate them have been undertaken.

The range of scores that are attributed to entities on the base of this factor is as follows:

- **0** = Risk management is not defined as a process;
- **1** = Risk management is defined as a process in a strict compliance with the Code of listed companies;
- **2** = Risk management is defined as a process in compliance with the Code of listed companies, but it appears more customized for the entity;
- **3** = Risk management is defined as a process in compliance with the Code of listed companies, but it appears more customized for the entity and it is exhaustively explained how this process works in the specific company and who are subjects involved.

ERM as a strategic and decisional system

A mature ERM is a process directly connected to the higher-level processes of the company.

Once that the strategic objectives for the firm are set, the BoD defines guidelines for risk management to maintain it aligned to the strategy. Indeed, the aim of the ERM process is to assure that the company is able to address its risks in order to deal with the strategic objectives set, to maximize shareholders' value and to satisfy other stakeholders. Therefore, already from the first step of this cyclical process, ERM is concatenated to other internal processes.

Furthermore, risk management contributes to the adoption of informed decisions that, based on a risk-return analysis, result consistent with the risk appetite.

Moreover, ERM is a process that permeates all business processes.

The range of scores that are attributed to entities on the base of this factor is as follows:

- **0** = ERM is not described as integrated with other company's processes;
- **1** = ERM appears integrated with other company's high-level processes in a formal declaration in compliance with the Code of listed companies;
- **2** = ERM appears integrated with other company's high-level processes in compliance with the Code of listed companies, but the description appears more detailed and customized for the entity.

Enterprise-wide scope

According to Segal (2011), ERM has to apply to each area of the entity.

Therefore, it should emerge from the official documents that the company is making many efforts in order to ensure consistency of this system within the entire organization, including all functional areas, businesses, and controlled entities.

In example, according to what reported in Enel's guidelines for the "Sistema di Controllo Interno e Gestione dei Rischi" (2016), "the Risk Control Unit has to ensure the efficient implementation at the Group level (holding plus controlled companies) of the process of identification, quantification, assessment, reporting and monitoring of risks".

The range of scores that are attributed to entities on the base of this factor is as follows:

- **0** = It is not declared within the report the presence of an enterprise-wide scope or it is declared that every department, business, controlled company is adopting a stand-alone system or that not all the entity's areas are involved/assessed within the ERM;
- **1** = The entity declares that an enterprise-wide scope is adopted;
- **2** = The entity declares that an enterprise-wide scope is adopted, and further information are provided.

Risk culture

Within a mature risk management system, all people who work for or with the entity are empowered to identify and manage risks, being the "owner" of the risk and the first level of control. Therefore, it results fundamental to create a good level of sensibility in people in order to ensure that they succeed in this role. However, specially for big/multinational companies that have operations and subsidiaries all around the world, it can be difficult to coordinate and align all these subjects to ensure consistency in the way in which they deal with risk.

Therefore, the spread of a risk culture and the work done by risk managers are fundamental to reach this objective.

The range of scores that are attributed to entities on the base of this factor is as follows:

- **0** = It is not threated in the official documents the theme of risk culture;
- **1** = It is cited in the official document the presence of a noteworthy risk culture;

- **2** = it is identified within the official documents the presence of a noteworthy risk culture and further information is provided.

Wideness of risk types assessed

In order to have a clear picture of risks present in the environment surrounding the entity and of the internal challenges that affect this latter, all risk categories require a good level of attention and consideration. According to Crouhy, Galai, Mark (2014), it is no longer sufficient to consider only past risk categories or those risks mainly related to the sector in which the entity operates.

The range of scores that are attributed to entities on the base of this factor is as follows:

- **0** = There is not evidence about risk assessment or it is described only for specific risk types (i.e. financial);
- **1** = A wide variety of risk categories is declared about the assessment done by the entity;
- **2** = A wide variety of risk categories is reported about the assessment and further information is provided.

Integrated way in managing risk

To avoid silo-approaches is one of the main prerogatives of a mature ERM.
Indeed, ensuring a good level of coordination among the different functions involved and providing them with good guidelines, it is possible to avoid the three main problems of the silo-approach: incompleteness, inefficiency and inconsistency.
Furthermore, to ensure information flows within the different parts involved would increase consistency and would create a more effective risk management system.

The range of scores that are attributed to entities on the base of this factor is as follows:

- **0** = There is no evidence that it is ensured coordination and consistency in the way in which different risks are managed;
- **1** = The level of integration in managing different risks is explicated;
- **2** = The level of integration in managing different risks is widely explicated and further information is provided.

Risk Committee

According to Segal (2011), the risk committee "has a primary role of defining risk appetite and risk limits, and managing enterprise risk exposure to within these tolerance limits".

Furthermore, other main responsibilities of the risk committee are:

- Review and approval of the ERM framework and of the early structure of risk governance;
- Review of risk identification process;
- Review and approval of the integration of risk management and other entity's processes as strategic planning and decision-making;
- Review and approve risk messaging.

However, italian listed companies are subject to the "Codice di Autodisciplina" that impose them to create a "Comitato Controllo e Rischi" (CCR) with a supporting function to the BoD. This committee (taken in consideration) is normally the closer structure to the risk committee, as intended by Segal (2011), and it has the same function (as listed above), but only with a support responsibility.

Therefore, on the base of the consideration above, the range of scores that are attributed to entities is as follows:

- **0** = The company has not a CCR or it does activities not aligned to the responsibilities above;
- **1** = The entity's CCR has responsibilities partially aligned to the definition above;
- **2** = The entity's CCR has responsibilities aligned to the definition above;
- **3** = The entity has a specific "Comitato Rischi" (to support the BoD), in addition to the "Comitato Controllo", with responsibilities aligned to the definition above.

CRO

The role of the Chief Risk Officer, introduced not more than 10 years ago, was initially diffused among entities operating in the financial sector.

Nowadays, the relevance of this function is increasing and also companies operating in different sectors are introducing it in their structure. Therefore, the presence of this C-suite role is considered another good key element to check the way in which the ERM is implemented into the entities part of this sample.

According to Segal (2011), responsibilities of the CRO are:

- Build and follow the ERM process, together with the ERM team, to ensure its functioning;
- Create buy-in to ERM and ensure recognition and participation within the company;
- Monitor and supervise that exposures are maintained within the risk appetites sets by the BoD with the support of the CCR;
- Be the point of communication and coordination with the other C managers.

On the base of the definition above, the range of scores that are attributed to entities is as follows:

- **0** = There is not evidence in the report of the presence of a CRO;
- **1** = The entity's CRO has responsibilities not sufficiently aligned to the definition above;
- **2** = The entity's CRO has responsibilities generally aligned to the definition above;
- **3** = The entity's CRO has responsibilities aligned to the definition above.

All people involved

The last key element assessed for each company is the involvement in risk management of people operating at every level and in every area of the organization. To ensure a proper ERM, it is needed a central function composed i.e. by the ERM team, the CRO, the Risk Committee and generally by all those committees empowered to enhance at a corporate level the output generated by the system. However, in order to ensure the identification and proper management of all risks, it is needed the participation of all people involved in the organization. Indeed, having a perfect knowledge of the business and of the specific department in which they operate, they are the best point of contact to obtain information about the emerging risks and to manage them. Therefore, after that the Risk Committee has set the risk appetite, through a top-down approach, it is communicated to each function and department the risk limit (Segal, 2011).

Furthermore, as stated in a research provided by the Institute of Internal Auditors (2015) about the Three Lines of Defense Model (widely threated in Chapter 2), are the front line operating managers to directly "own and manage risk and control".

The range of scores that are attributed to entities on the base of this factor is as follows:

- **0** = Risk management appears in the Corporate Governance Report still perceived as the responsibility of a small group of people;
- **1** = In the Corporate Governance Report all people are declared responsible;
- **2** = As declared in the Corporate Governance report, all people are involved, and it is described how the 3 Level of Defense Model is applied in the company.

Once that the key elements and their relative scores have been defined, it is now possible to assess the level of implementation of the risk management system of the entities in the sample. Thus, after a careful analysis conducted within the official documents of firms, it has been possible to extrapolate data needed and to assign them a score.

In table 1.2 are reported the results obtained from the research conducted. In all columns, except for the last one, there are the partial scores for each element, and in the last column is shown the sum of the partial scores. On the base of this last column, entities have been ranked from the one that totalized the biggest score, meaning that it has "expressed" the most mature risk management system, until the one with the lowest score, meaning that the "declared" level of implementation of the system is lower.

Furthermore, in the last row are shown the average score totalized for each key element. This additional row has been added in order to check which are the factors that most easily have been implemented and which are those still requiring many efforts by entities.
Red cells identify elements whose average is lower than the mean of the possible scores attributed to them, orange cells identify elements whose average is a bit higher than the mean of the possible scores attributed, and green cells identify elements whose average is greater than the mean of the possible scores attributed.

Before proceeding with the assessment of results, it is important to remember that this study is conducted on the base of what companies have reported in their Corporate Governance Reports. Therefore, assessments have been done on the base of entities' declarations.

Table 1.2: *Assessment of the level of implementation of ERM*

Entity	Process	Integrated process	Enterprise wide scope	Risk culture	Wideness of risk types assessed	Integrated way in managing risks	All people involved	Risk Committee	CRO	Tot
ENI	3	2	2	2	1	1	2	3	2	**18**
Intesa San Paolo	1	2	2	1	2	2	2	3	3	**18**
FCA*	3	2	2	2	2	2	2	3	0	**18**
Generali	1	2	2	2	1	2	2	1	3	**16**
Unicredit	2	2	2	2	1	1	2	2	2	**16**
CNH Industrial	3	2	2	0	2	2	2	1	0	**14**
Autogrill	3	2	2	1	1	2	2	1	0	**14**
ENEL	1	2	2	2	1	2	2	1	0	**13**
Telecom Italia	3	2	2	0	1	2	1	2	0	**13**
Brembo	2	2	2	1	1	1	2	2	0	**13**
Credito Emiliano	2	2	2	0	0	2	2	3	0	**13**
Terna	2	2	1	0	1	2	1	2	1	**12**
Snam	3	2	2	0	1	1	2	1	0	**12**
Poste Italiane	1	2	1	1	1	2	2	2	0	**12**
De' Longhi	2	1	2	0	2	2	1	1	0	**11**
Luxottica Group	2	1	1	0	1	2	1	1	1	**10**
Exor	3	1	1	0	1	1	2	1	0	**10**
Acea	1	1	1	0	2	2	2	1	0	**10**
Atlantia	2	0	2	2	0	0	0	2	1	**9**
Amplifon	2	2	2	0	1	0	1	1	0	**9**
Banca Generali	1	1	1	0	0	1	2	2	0	**8**
SIAS	3	1	1	0	1	1	0	1	0	**8**
Hera	1	0	1	0	2	0	1	2	0	**7**
Inwit	1	1	1	0	1	0	1	2	0	**7**
Ansaldo STS	2	1	1	0	0	0	0	2	0	**6**
Recordati	1	0	1	0	0	1	1	1	0	**5**
Parmalat	1	1	0	0	0	0	1	1	0	**4**
Diasorin	1	0	1	0	1	0	0	1	0	**4**
Ima	1	0	0	0	0	0	0	1	0	**2**
Tenaris**	0	0	0	0	1	0	0	1	0	**2**
Average	1.86	1.34	1.45	0.55	0.97	1.17	1.34	1.60	0.43	
Mean	1.5	1	1	1	1	1	1	1.5	1.5	

* Being FCA subject to Dutch authority in terms of corporate governance regulation, the responsibilities identified for the Audit Committee (Comitato Controllo e Rischi) are slightly different from those identified by the Italian authorities. When valuing FCA on this element, the definition of Segal (2011) for the responsibilities attributed to the risk committee is applied.

**The Corporate Governance report was not available for Tenaris. The assessment has been apparently conducted on the base of partial information.

1.4.5 Comments on the research

On the base of the research conducted, there are two kinds of considerations to be done.
The first one is an assessment of the key elements singularly taken and of their averages, the second one is a consideration about how companies rank in the list and about possible rationales behind it.

1.4.5.1 Comments on key elements

This first kind of comments has a huge relevance in order to identify those elements on which entities focused the implementation of their risk management system and those that, instead, still require many efforts to be implemented. Indeed, as can be observed in table 1.2, there are some factors that scored well and others that, among the majority of the entities, scored bad. It is a clear sign that the level of attention given by companies, as well as by authorities, that require entities to disclose information related to these factors, is still low.

ERM as a process

The "Codice di Autodisciplina" of listed companies refers to the basic elements of risk management/control system as a process that runs through risk identification, risk assessment, risk decision-making and risk monitoring and is included in a wider system.
Many entities have reported in their official documents only this essential definition without adding other information about how the process is ran. Therefore, companies that scored 1 for this factor generally seem to be only in a formal compliance with the basic elements of the Code, failing to explain and, maybe, actually implement the entire process.
Instead, entities that scored 3 appear to have a risk management system that not only comply with the Code, but that is also presented and implemented in a personalized way.
Furthermore, almost none of the entities scored a 0 for this factor, meaning that at least they complied with what required by the Code.

One of the companies that better scored in considering ERM as a process is ENI. Indeed, this firm not only defines the process as continue, integrated, interactive, monitored, and developed by people, but it also exhaustively describes the different phases of the process, the different

subjects involved and how, for every phase, the system is integrated with and permeates other processes.

Looking at table 1.2, it is possible to observe that the average obtained for this element is higher than the mean. Thus, even if some entities still need to make efforts to implement risk management as a process, this value is quite satisfactory. Furthermore, it can be observed again from table 1.2 that financial entities have not scored the best for this factor.

ERM as a strategic and decisional system

Once that we have assessed that almost all entities consider the risk management as a process, we can observe that the majority of entities also consider it as integrated in the structure of the entity it-self. Furthermore, as is shown in table 1.2, more than half of the companies that consider risk management as an integrated process provided examples and described in a personalized way how their systems are integrated with all the other processes of the company.

Moreover, almost all entities that scored a 2 are also in the first half of the list, meaning that all companies that scored well in total gave a good level of attention on this factor.

Companies as Autogrill and Enel express their efforts in integrating risk management in decision-making, while Terna identifies the integration of risk management with strategy setting and budgeting. Furthermore, Poste Italiane expresses how, through the use of a risk-return assessment, the company takes conscious and informed decisions.

Enterprise-wide scope

As shown in the last row of table 1.2, this key factor scored quite well among all companies. Indeed, the average results greater than the mean and only three entities failed to consider the enterprise-wide scope of the system.

Almost all entities affirm that their risk management activities are intended to apply to the entire group (considering also subsidiaries) and to every business and department they have, ensuring coordination and the application of the same rationale in managing risks.

Those entities that scored 2 add in their declarations additional information about the way in which they do it. In example, Intesa San Paolo and Credito Emiliano underline that the risk appetite is set for the entire group and that risk limits are then provided for each department. Generali attributes, instead, to the figure of CRO the responsibility in coordinating the different departments/businesses/subsidiaries in managing risks.

Risk culture

Risk culture is one of the key factors for which companies show a low level of attention.
It is not something on which the Code appears strictly focused, but it is an element that would surely enhance the success of the system. Therefore, even if it is not mandatory for entities to develop a strong risk culture and declare it, it is important that they ensure, for the good result of the system, that all people involved are committed to and acknowledged of the way of managing risks.

More than half of the entities fail to declare the presence of a risk culture and only six, out of the ten that recorded a value higher than 0, provide additional information about the way in which the risk culture is developed.
Companies as ENI and Atlantia identify the roles, respectively the “Responsabile Risk Management Integrato” and the “Amministratore Incaricato del SCIGR”, to which is assigned the responsibility to ensure that a good risk culture is developed within the company.

The development of a risk culture should be at the base of every risk management system to ensure a good level of buy-in to the system. Indeed, if a company fails to ensure that the right people participate to risk management, even having a well structured framework to manage risk, the entity would fail in its objectives.
Therefore, it is one of the key elements for whose development companies have to work the most.

Wideness of risk types assessed

A mature ERM system should involve the assessment of all risk types. Unfortunately, as can be observed in table 1.2, the average for this key factor is lower than the mean.

Furthermore, even if the majority scored a value higher than 0, very few entities succeeded in providing a dynamic presentation of risks types different from just saying that all risk categories (strategic, financial, operational, ..) have been included.

Moreover, as can be observed by the way in which they disclose information, many entities, specially among those of the FTSE ITALIA MID CAP, failed in providing sufficient attention in their assessment to risk categories different from the financial one. Indeed, exhaustive explanations are given in relation to the functioning of the "SCIGR in relazione al processo di informativa finanziaria", but the same accuracy in description is not ensured for the assessment involving other risk types.

Among companies that scored the best we can note that FCA, De' Longhi and Acea provide a detailed list of the main risks including also an exhaustive description of the risks and of the ways to manage them.

Integrated way in managing risk

According to the scores reported in table 1.2, entities have not well expressed how they manage risks in an integrated way. The relevance of this factor has already been expressed in paragraph 1.3, but entities seems not to have caught this importance.

Those companies that scored a 1 generally have a second line of defense, represented by the risk management function, that has the objective to ensure coordination and consistency in the way in which the risk owners manage risk. Instead, those entities that scored 2 provided information on the way in which they ensured integration in managing different risks.

Among the entities that scored well we find Intesa San Paolo that sets continuous information flows among the parts involved and ensures coordination in the identification of actions to manage risks.

Furthermore, also in this case, it is possible to observe that those companies that scored the highest value are ranked in the first half of the list. Therefore, even if the relevance of this aspect has not been well emphasized by the entire sample of companies, entities that ranked the best have focused their risk management system also on this element.

All people involved

As can be observed in table 1.2, entities disclose in their Corporate Governance Report important information in relation to the positive participation of all people to risk management. Therefore, the average value results higher than the mean.

Almost all companies that are part of the FTSE MIB basket, with the exclusion of Telecom Italia and Luxottica Group that score 1 and of Atlantia and Tenaris that score 0, disclose information about the three lines of defense they adopt in managing risk and, therefore, about the participation of every person to the first line of defense. People directly working in the department are considered "risk owners", and they are directly involved in managing risks arising during the operating activity.
Entities that are part of this basket appear, then, more focused on adopting a system of control that is based on different lines of supervision in order to assure the achievement of corporate goals.
Instead, the majority of companies that scored a 0 or a 1 are part of the FTSE ITALIA MID CAP.

However, criticism may arise if we observe the negative results obtained for risk culture and the positive ones obtained for this element. Indeed, a spontaneous question would be: "how can entities ensure that everyone is committed to risk management, if a risk culture is not diffuse within the company?".

Risk committee

As already stated in paragraph 1.4.4, in order to comply with Italian regulation for listed companies, the BoD has to create a "Comitato Controllo e Rischi" that has a supportive function to the BoD it-self.
Within this research, more than the risk committee as defined by Segal (2011), has been observed the presence of and the way in which the CCR works.

In this case the average obtained is quite aligned with the mean. However, it is a more than positive sign if we consider that companies could score a 3 only if the specialized "Comitato Rischi" was divided by the "Comitato Controllo". Therefore, a value equal to 2 is an indicator of the good

presence of a committee that has a supportive function in creating and implementing a risk management system, in determining the risk appetite and the risk tolerance and in integrating the system with the other processes of the company.

It is important to note that three out of the four that score a 3 are first in the list.

CRO

This last key element is also the one that scored the worst. Indeed, only seven out of the thirty entities declared in their corporate governance reports the presence of a Chief Risk Officer.
Furthermore, only four of them (these four are also among the first five of the list) scored a satisfactory value higher than the mean.

Another important aspect to note is that the majority of the entities that reported the presence of a CRO are financial entities (specifically Intesa San Paolo, Generali, Unicredit and Credito Emiliano). Therefore, in this specific sector, more than in the others, entities consider the institution and the disclosure in their official documents of a CRO a relevant aspect to implement a good risk management system. Thus, the result of this research confirms what previously affirmed in paragraph 1.4.4: the role of the CRO has firstly been introduced in the financial sector and is now gaining a bit of space also in other sectors.

Final general comments

In conclusion, after having assessed on a single-base every key element, it is possible to observe that even if companies recognize the relevance and the benefits of implementing an ERM system, the majority of them is still not able to fully implement it.
Indeed, the biggest part of this sample appears more focused on formally comply with the directives rather than on making efforts to actually create and structure a good risk management system.
It is not a surprise then that the elements that recorded an average higher than the mean were exactly those more regulated and for which entities were obliged to disclose information in order to comply with the Code.

Only 9[1] out of the total number of entities part of the sample refer to their risk management system as ERM. It is important to consider that only 6 of them are among the first 10 and that none of them is a financial entity.

1.4.5.2 Comments on entities' score

The aim of this paragraph is to assess if the order of the entities in the list has been influenced by specific drivers, as the size or the sector of activity of the company. For the scope of this research, it is a fundamental point. Indeed, to understand the reason why some companies have reached a better level of implementation than others would provide an improved level of understanding of the results obtained.

Looking at table 1.1 (where it is possible to observe the characteristics of every company) and at table 1.2 (where it is possible to observe how they ranked), it can be noted that the size of the entity played an important role in determining the maturity of the risk management system. Indeed, if we set **12**[2] as satisfactory threshold for the total level of implementation, we can observe that 11 out of the 14 companies that scored above the threshold are part of the FTSE MIB basket.
Therefore, bigger is the company and greater is the available capital, and more mature will result the risk management system, being the company more able to invest to implement a better structure to manage and control risks. Furthermore, bigger and more complex is the company and greater will be the willingness and the need of the company it-self to develop a greater risk management system to manage all those events that would create deviations from expected and to let the company continue to perform well enhancing its value.

Another element that played a big role in determining this ranking is the macro-sector in which entities operate.
Indeed, as can be observed in graph 1.2, basing the assessment always on a **12** threshold, almost all entities operating in the financial macro-sector (5 out of 7) have implemented a good ERM.

[1] Entities that define their risk management systems as ERM are: Luxottica, SNAM, Telecom Italia, CNH Industrial, FCA, Hera, De' Longhi, Brembo and Autogrill. Furthermore, ENI defines its system "Risk Management Integrato".

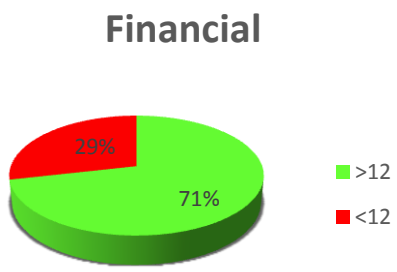
[2] The threshold is set considering the first value higher than the mean of the total amount that companies can score.

Financial entities, as banks and insurances, are subject to further regulations that impose them to implement their risk management system also on the base of additional requirements and details.

As shown in graph 1.3, entities operating in the utility sector, that in this graph includes also ENI, record mature risk management systems. Indeed, the ERM of 4 out of the 6 entities totalized a score greater than the threshold.

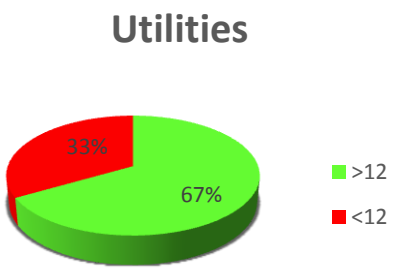
Considerations about financial and utilities macro-sectors resulted specifically relevant. However, through the observance of graphs 1.4, 1.5, 1.6, 1.7, 1.8 and 1.9, it is possible to identify, also for companies operating in other areas, the level of influence that the macro-sectors had on the implementation of the risk management systems of the remaining entities.

Graph 1.2: *ERM's score of financial entities*



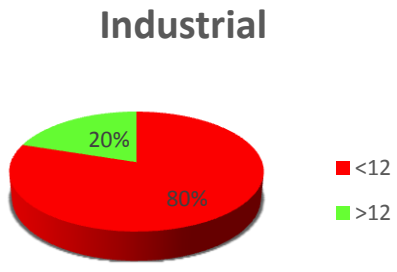
[ERM of 5 out of the 7 financial entities score >12]

Graph 1.3: *ERM's score of utilities entities*



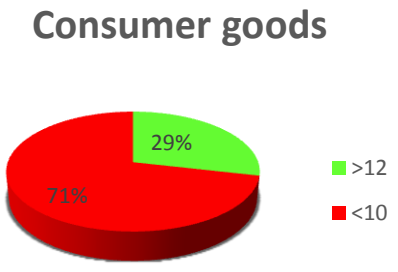
[ERM of 4 out of the 6 financial entities score >12]
For this graph, ENI has been considered as utility.

Graph 1.4: *ERM's score of industrial entities*



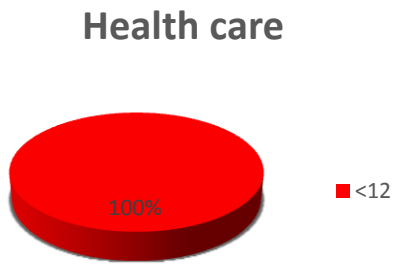
[ERM of 1 out of 5 industrial entities score >12]

Graph 1.5: *ERM's score of consumer goods entities*



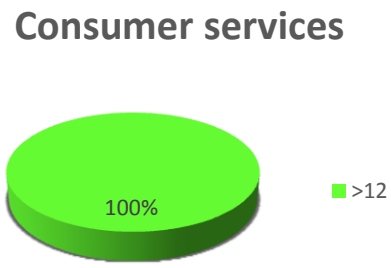
[ERM of 2 out of the 5 consumer goods entities score >12]

Graph 1.6: *ERM's score of health care entities*



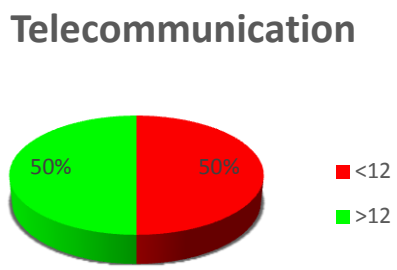
[ERM of all (3) health care entities score <12]

Graph 1.7: *ERM's score of consumer services entities*



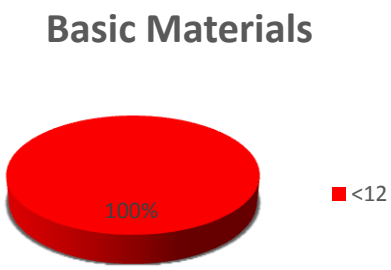
[ERM of all (1) consumer services entities score >12]

Graph 1.8: *ERM's score of telecommunication entities*



[ERM of 1 out of 2 health care entities score <12]

Graph 1.9: *ERM's score of basic materials entities*



[ERM of all (1) consumer services entities score >12]

According to what emerged from this research, the last element that has an influence in the level of implementation of risk management is the presence of the entity in foreign markets.

Indeed, taking as sample ENI, it is possible to observe that the company took many of its practices in managing risks by foreign best practices. As reported in their annual report, being the company a multinational also listed in the NYSE, partially because of the necessity to comply with the foreign regulation and partially because of the willingness to improve its risk management system, ENI continuously adapted its process in order to embed all foreign best practices.

Therefore, the geographic scope can positively influence the risk management maturity.

2. Risk governance – roles involved

2.1 Risk governance

In every company, association, family are identified best practices or activities that allow getting the best results and ensure comfortably proceeding, day after day, in the ordinary management. However, setting these activities will not ensure reaching the defined objectives, if the company, association or family fails to identify, who is the person responsible for the activities' execution.
In example, thinking at a family, we might identify as best practice that children are controlled and protected in order to ensure their good and healthy development. However, could be imagined that this activity is executed by a 3 years-old child over the 9 years-old brother? Obviously not. Normally, it is responsibility of parents to ensure the protection and the care of their children.
Therefore, the same logic can be applied in a more complex entity's context. Once that best practices are identified, in example, roles and responsibilities need to be attributed.

Speaking about risk management, according to Segal (2011), the ERM infrastructure is constituted by two elements: the ERM framework and the risk governance.

The first element provides the "functional structure", representing all flows and activities that need to be done to ensure a proper risk management system able to provide assurance on the achievement of corporate's objectives. Specifically, it identifies:

- **What** are the activities and best practices that need to be put in place;
- **How** do they interact within each other and how do they ensure an integrated system;
- **Why** are they performed.

Risk governance provides instead the "hierarchical structure", identifying how roles and responsibilities within ERM are settled, divided and assigned to people part of the organization.
Specifically, it identifies:

- **Who** has the responsibility to perform a specific activity;
- **When** is the right time during the ERM cycle to perform that specific activity;
- **Where** these activities take place.

According to what reported in the Risk Governance Guidance for Listed Boards issued by the Corporate Governance Council (2012), "Risk governance is the architecture within which risk management operates in a company". It ensures a suitable level of control on the implementation and execution of the activities needed to identify, assess, mitigate and message risks. Therefore, it is fundamental to ensure that company's goals are pursued and that all the actors involved properly participate in managing risks.

According to Renn (2008), looking at the complex web of actors involved in managing risks, Risk Governance is of specific relevance in situations where is required collaboration between these actors. Indeed, in setting roles and responsibilities, a proper risk governance would also identify how the different actors cooperate and participate to the process.

This chapter focuses on risk governance and goes deeper in identifying the main subjects involved (according also to the Italian Code for listed companies) and their specific roles. Furthermore, particular attention is given to the Three Line of Defense Model.

However, before that the different roles and responsibilities are described and identified, it is worthy to say that it is not possible to make generalizations on how risk governance is implemented in the organizations. Indeed, according to Segal (2011), it has to be customized for every different entity; and two are the main reasons for it.

Firstly, as was also observed by the research conducted in chapter 1, every organization implements and structures its ERM system focusing on some aspects more than others and deciding to execute some activities rather than others. Therefore, being risk governance the architecture that allows the different activities to take place, it will not be possible to determinate the same roles and structure for every organization, if the activities they perform to manage risks are different. Risk governance has to be defined around the ERM activities identified.

Secondly, every entity has already in place a governance process and, in order to ensure efficiencies and to let the ERM process permeate all other organization's processes, entities conduce risk governance readapting/through the governance processes already in place. This fact will cause organizational structures not to be the same for every company, and it is another explanation of why it is not possible to generalize on them.

However, according to the regulation for listed companies and to specific codes, some roles of the risk governance are common for all the entities, even if with some differences in their responsibilities.

In the following paragraph are identified these roles and their respective responsibilities.

Before proceeding, it is important to underline again that specific regulations are developed according to the sector where the entity operates. In describing the main roles involved in risk governance for Italian listed companies, there is full awareness that some differences might arise when considering financial entities. Therefore, when these differences arise, additional information are provided for these entities.

2.2 Main roles & related responsibilities in risk governance

In the last decades, internal control systems acquired a new meaning and evolved becoming an integrated management tool embedding risk management. Therefore, when the main roles involved in risk governance are investigated, answers are found in the main actors of the corporate governance systems.

Italian listed companies put in place the "Sistema di Controllo Interno e di Gestione dei Rischi (SCIGR)" that is defined, according to the Codice di Autodisciplina (art. 7.P.1), or "the Code", as the group of rules, procedures, and structures aimed to the identification, assessment, management, and monitoring of the main risks. Therefore, to figure out who are the actors involved and which are their responsibilities in risk governance, this thesis focuses on the subjects involved in the SCIGR and reports their responsibilities according to the Italian legislation.

According to the Principle 7.P.3 ("the Code") that identifies the main actors involved in the SCIGR and to the "Criteri Applicativi" from 7.C.1 to 7.C.6 ("the Code") that provide a deep description of these actors, below are presented the main roles and responsibilities.

<u>Board of Directors</u>

The main role of the Directors is to manage the company ensuring that its strategy and objectives are achieved, as ruled by the art. 2080-bis of the Italian Civil Code.

Risks might prevent the BoD from the accomplishment of its responsibilities, having a potential negative impact on the entity and its businesses. Therefore, with the greater awareness of risk and of the positive effects of risk management developed in the last years, is attributed to the BoD also a central role in the SCIGR and in the risk management cycle.

According to "the Code" ("Criterio Applicativo" 7.C.1 - lett.a), the BoD defines guidelines to design and implement a SCIGR that is able to identify, measure, manage and monitor the main risks affecting the entity and its subordinated.
In performing this activity, the BoD should consider the structure of the company, the size, the sector in which it operates, and the regulation that is applied to it. Indeed, these elements would allow the Board to implement a system that, still complying with the legislation, is customized for the entity and ensures the achievement of its specific objectives.

Furthermore, the BoD has to define the nature and the extent of risks that the organization might undertake compatibly with its strategic plans ("the Code", CA 1.C.1).
This activity generates the starting point for the risk management activities performed by all the subjects involved. Indeed, once that the risk appetite is defined, risk limits are derived and communicated to the different roles and functions involved with a top-down approach.
The application of the appetite and of the different limits is then required through:

- Definition of strategic, operative and financial plans in line with the level of risk that the organization can undertake;
- Management of risks at a functional and corporate level aligned to these limits and appetite.

In relation to the Risk Appetite Framework, it has to be highlighted that Banca D'Italia provides for the bank sector a much wider set of rules for the determination of the RAF.

Moreover, at least annually, the BoD evaluates the adequacy of the SCIGR to guarantee its alignment to the characteristics of the company and to the level of risk adopted ("The Code", 7.C.1 – lett.b).

In addition, the BoD approves the corporate structure and the governance system chosen by the entity. It provides a clear definition of roles and responsibilities, avoiding conflicts of interest and

ensuring coherence with the business model adopted and the activity performed (Banca D'Italia, Circ. 285 17/12/2013).

Moreover, the BoD is responsible for the supervision of the communication between the organization and the stakeholders. In this role, the Board has to ensure transparency and disclosure of the facts and figures related to the entity and has to ensure that risk is messaged. This supervision is important to create a risk management system that, after having identified, assessed and managed risks, is also able to disclose the relevant information to the subjects involved (Banca D'Italia, Circ. 285 17/12/2013).

Among the activities performed by the BoD, there is also the approval of the Audit plan proposed by the responsible of the Internal Audit function ("the Code", 7.C.1 – lett. C).

According to what is stated in "the Code" (4.P.1), the BoD creates internally one or more committee that have proactive and consultative functions to the BoD. These specialized committees, then, provide technical support to the Board when taking decisions in their specific areas.

<u>Comitato Controllo e Rischi (Audit Committee)</u>

The Comitato Controllo e Rischi has a consultative function to the Board and it is addressed to ("the Code", 7.C.2.):

- Validate the correct use of financial standards in redacting the financial statements and the financial information communicated to the public.

  This activity not only ensures that financial information are correctly produced, but also that the communication with stakeholders is transparent and, in case risks arise, they are promptly communicated.
- Assess and express judgements on aspects related to the process of identification of risks. According to Stella Richter, this committee has not only a consultative function. Indeed, in expressing its judgements it ends with participating to the design, creation and management of the SCIGR.
- Periodically refer to the Board of Directors in relation to the appropriateness of the SCIGR. The committee continuously monitors the activity conducted by the SCIGR. Through this

control, it ensures that the system is aligned to the business model adopted by the organization and that it is properly working to maintain the level of risk within the risk appetite and to allow the entity to reach its strategic objectives.

- Assess the periodic reports produced after evaluations of the SCIGR and the reports produced by the Internal Audit function.
- Monitor the autonomy, the appropriateness, the effectiveness and efficiency of the Internal Audit function. Furthermore, the CCR may also ask the Internal Audit to conduct audit activities on specific areas.

The Codice di Autodisciplina does not impose organizations to create a CCR internal to the BoD. Indeed, according to the dimension of the company and to the specific environment and situation, the Board might decide to divide the roles normally performed by the CCR and assign them directly to the directors. Sometimes, organizations might also opt to adopt a single committee rather than three committee (Comitato per le Nomine, Comitato per la Remunerazione, Comitato Controllo e Rischi) as recommended by "the Code". In this latter case, the single committee will have competences and responsibilities in all the different areas. However, this option has to result coherent with the characteristics of the entity.

Director of the SCIGR

According to "the Code" (7.C.4.), the Director in charge of the SCIGR has an important role in risk governance and many relevant responsibilities are attributed to him.

As already said in the previous chapter and as will be better explained later on, managers are considered "risk owners", being the one directly operating in the area/business/department and, therefore, being the most suitable to identify and deal with the related risks.
Once that this is defined, it has to be considered that companies might be wide entities and that risks faced might be numerous. Then, it is needed a person that cures the risk identification within the wide organization and, after having highlighted the most relevant risks, presents them to the Board. This role is attributed to the director of the system.

Furthermore, once that the BoD defines the guidance for the SCIGR, he has to implement them to ensure that the system has been correctly designed and created and that it is efficient and aligned to the structure of the organization and to the guidelines of the Board.
Moreover, in executing this directives, he acts to assure that the system is aligned to the new practices and regulation and to the operative situation of the entity ("the Code", 7.C.4.).

The director of the system has the duty to promptly address the Audit Committee (that in turn will refer to the Board) or directly the BoD the emergence of issues or major risks in its activities or in the system, so that the Committee or the Board are able to address them.

Moreover, as the Audit Committee, this Director might request to the Internal Audit function to execute specific audit activities on sensitive areas or aspects of the system.

Chief Risk Officer (CRO)

Another important actor that takes part to the risk governance is the Chief Risk Officer.
This figure, whose role is not defined in the Codice di Autodisciplina, is meant to be a dedicated figure not directly involved in the business and different from the Internal Audit function. It provides the entity with objective considerations on the company risk profile and on the mitigation actions undertaken (Quaderni Assirevi, 2016).

The CRO is the bonding point between the risk management system and the Board and all the high level and C-Suite level managers. An important responsibility of the CRO is to contribute at the diffusion of the risk culture within the organization and to ensure the involvement of employees to the system.

Moreover, having an external objective point of view, the Chief Risk Officer ensures coordination between the risk owners, the risk management function and the Board through the continuous support and guidance provided during the risk assessment and the aggregation of its results and, then, during the identification of the related mitigation actions. In this latter activity, it might intervene in the decision of the different mitigation options.

Therefore, its role should then be to exercise an overall control over the risk management system and to intervene when it is needed, and not necessarily to manage specific risks (Quaderni Assirevi, 2016).

The role of the Chief Risk Officer would be specifically beneficial in organizations having a structural complexity and a high risk profile. Indeed, it would provide its objective and experienced suggestions and would facilitate the interactions between the subjects part of the complex structure.

As might be noted since here, the subjects involved in risk governance are many and they all have to report to the BoD that, according to the Civil Code, is responsible for the management of the entity.

Furthermore, another point worthy of notice is that they are independent actors, but they are also extremely interconnected among them. Indeed, the key that let the entire control and risk management system work are the information flows and the coordination methods. Indeed, all these actors are pieces of the same engine and it is not possible to make it work if they do not collaborate within each other.

The next chapter will be entirely dedicated to this important topic and it will address in the specific the role of the Internal Audit in Risk management and the forms of coordination Italian listed companies have implemented.

Before proceeding with this topic, the chapter continues to describe the roles involved in risk management through the definition of the Three Lines of Defense Model and of the roles of “risk owners”, risk managers, and internal auditors.

2.3 Three Lines of Defense Model

According to Dittmeier (2015), to ensure an efficient corporate governance system, the risk management system and the internal control system should be integrated.

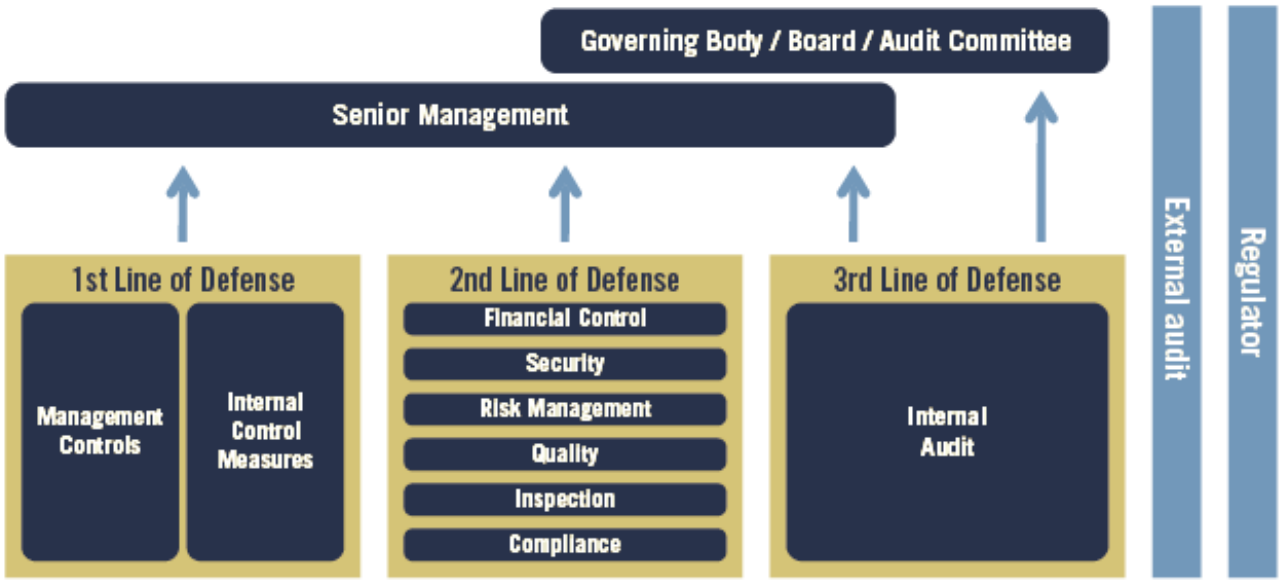
The finalization of control activities is to ensure that risks are properly addressed and that apposite procedures, mechanisms and solutions are found to contain them. These control activities are executed at all the hierarchical levels from the different functions involved.
It is evident the need to ensure the take on board of people working in different areas/levels of the entity and having various backgrounds and specializations, to create a system that is able to dial with the different risks and challenges faced.

A reference model is the Three Lines of Defense Model, inspired at the Corporate Governance Principles of Basilea. The Model that has been adopted by the Codice di Autodisciplina defines a control system structured on three different levels.
The Model gives an easy and effective method to increase communication on risk management and control through the definition of specific roles and responsibilities. Indeed, it not only involves the participation of different subjects, but it also defines how duties could be assigned and coordinated within the entity, independently of its complexity or size (IIA,2013).
When the lines of defense are properly implemented, it should be reduced the possibility of gaps in control and of duplication actions, and there should be a greater probability to proper address and manage risk and control. Moreover, it would be less likely that the Board receives biased data about the greatest risks affecting the entity and about how management is addressing them (IIA, 2015).

As can be evinced by the name, the Model is structured on 3 lines of defense, each composed by subjects/functions operating at a different level in the organization and addressing the risk using a different experience and point of view.
The first line of defense is constituted by the operational managers, the different risk managers and compliance oversight functions compose the second line, and the third line is composed by the Internal Audit function that provides an independent assurance.
Under the supervision and guidance of the BoD and senior management, these three necessary groups act within the entity to effectively manage risk and exercise control.

Before proceeding with a specific description of the Model, its structure is shown in figure 2.1.

Figure 2.1: *The Three Lines of Defense Model*



Source: *IIA Position Paper on the "Three Lines of Defense in Effective Risk Management and Control" (2013)*

According to what stated in the Position Paper of the IIA (2013), even if the Senior Management and the Governing Body are not directly included in the model, in order to make a complete discussion on risk management, it is important to dedicate some lines to them and consider their role.

As is shown in the figure 2.1, they are the first clients served by the Three Lines of Defense Model and they are also the best actors to ensure that this model is actually implemented within the organization. Moreover, Senior Managers have the last responsibility for the results of the first and second line and have to completely support the development of strong governance (IIA, 2015).

2.3.1 First line of Defense

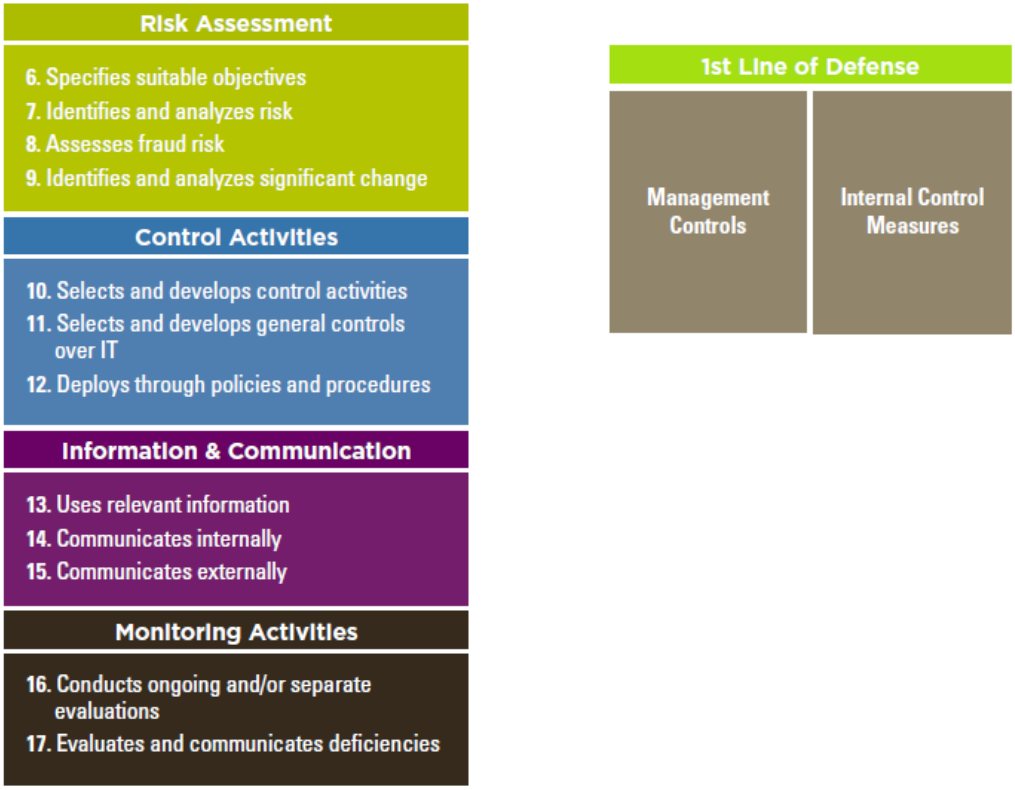
Operational managers, who directly own and manage the risk, represent the first line of defense. Their everyday activities create the risks that might represent an opportunity or a damage for the company preventing it from reaching its objectives. Therefore, they own the creation and implementation of remedies to contain and manage these risks.

Front-line and mid-line managers are involved in the everyday activities executed by their function and they result to be the most suitable people to maintain effective internal controls and to execute risk management activities on a day-to-day basis. Indeed, they are the first point of contact for all the new issues that arise and they are the first who might notice the insurgency of a deviation from expected.

According to what stated in the Position Paper of the IIA (2013), "Operational management identifies, assesses, controls, and mitigates risks, guiding the development and implementation of internal policies and procedures and ensuring that activities are consistent with goals and objectives".
Through the adoption of a top-down approach, the mid-line managers create detailed procedures that function as guidelines that their employees should use in executing risk management.

In figure 2.2 it is possible to identify which are the activities, among those activities identified by the COSO Framework, performed by the first line managers.

Figure 2.1: *The Three Lines of Defense Model*



Source: *"Leveraging COSO across the Three Lines of Defense", IIA (2015)*

2.3.2 Second Line of Defense

From what described above, the first line of defense might appear sufficient to manage risks through the 12 activities identified by the COSO Framework. However, it is important to underline that companies might have a complex structure and a wide number of functions, activities and operations. As described in chapter 1, one of the core elements of ERM is the implementation of a system that makes considerations and takes decisions at a corporate level on the base of aggregated metrics. Therefore, for this kind of system is fundamental to ensure coordination among all the subjects who own the risk and mitigate it.
The responsibility of the second line of defense is then to assure that the objectives above are met.

To monitor and support the first line of defense, management creates in the entity dedicated functions. According to the size, the industry and more generally to the characteristics of the organization, these specific functions might be (IIA, 2013):

- Risk management function that makes easier the implementation from the operational managers of proper risk management practices and helps the risk owner to apply the risk limits defined through a top-down approach and to diffuse the relevant risk related information to the subjects involved in the system;
- Compliance function that has the duty to monitor the different risks and activities executed by the risk owners, ensuring that the entity results in compliance with the regulations.
- Controllership function that is responsible to control all the aspects related to the financial data, including the standards that have been used and the way in which these data are reported internally and externally.

As already said, the presence of all these functions is extremely dependent on the characteristics of the organization. In example, listed companies normally establish all of them; small companies instead might create a single second-line function that embeds all the different responsibilities (IIA, 2015).

These functions are management level functions and, even if they appear to be a bit more independent and external from the specific function, they are still under the monitoring of senior managers.

Looking at their main responsibilities, their general duty is to ensure that the risk owners have properly implemented risk management practices and, following the guidelines provided by the BoD, are collaborating to establish a risk management system that acts at the enterprise level and that is coordinated among the different functions and businesses.
According to what stated by the IIA (2013,2015), other main responsibilities of the second line are:

- Alerting the first line on the emergence of criticalities in the system and provide them with solutions and suggestions to the issue;
- Provide the first line with the risk management framework and with guidelines on how to implement proper risk management practices that ensure consistency of the system at the corporate level and avoid the creation of silos approaches;
- Identify and communicate to the first line any change in the risk appetite defined by the organization;
- Monitor the appropriateness in reporting, controls and compliance with regulations.

Risk management

"The aim of the Risk Manager is to promote, at all levels, the activity of risk management, with growth in the responsibilities taken on by all staff in respect of specific policies of watching over risk" (ANRA, 2011).
Risk managers act as bonding point between the BoD and the entire organization in terms of risk management. Indeed, they are able to satisfy the requirements of the Board by helping the staff and the risk owners to implement best practices aimed at mitigating the exposures to negative events and at taking advantage of and exploiting profit opportunities. Through monitoring and providing support and training, risk managers assure that the entire system works properly and that the strategic objective of the Board are achieved.

Risk managers are experts who know the internal and external environment in which the entity operates and, being the one responsible for the risk management system, have to ensure the creation of a system that is aligned with the emerging aspects and needs.

Furthermore, being experts and having transversal skills, they can promptly help the risk owners in identifying risks and the best solutions to manage risks that might influence different areas and businesses of the entity.

According to Banca D'Italia (Circ. 285, 2013), the major responsibilities of the risk management function are:

- Involvement in the definition of the Risk Appetite Framework, of the risk governance and of the different phases composing the risk management process;
- Assessment of the adequacy of the RAF;
- Assessment of the adequacy of the risk management system;
- Develop and maintain risk assessment methods, ensuring that many different risk scenarios are used and that risks correlation is considered;
- Develop and apply indicators able to track anomalies and inefficiencies in the system of assessment and control of risks;
- Monitor the risk level undertaken by the organization and its coherence with the risk objectives previously defined;
- Monitor that the risk level attributed to the different functions are respected.

In conclusion the second line functions, being management functions, might directly intervene in the modification and implementation of risk systems. This intervention ability prevents them from providing completely independent and objective assessments and judgements to governing bodies about risk management.
There is the need then for a third line of defense to provide completely objective assessments and proposal of solutions.

2.3.3 Third Line of Defense

Internal audit is defined by the IIA as an "independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes."

According to the definition above, differently from the actors involved in the previous two lines of defense, the internal audit function is able to provide independent opinions and assessments. Indeed, this function is not under the control of the senior managers, it is instead an autonomous player that is generally extern from the organizational structure in place within the entity and has to respond only to BoD.
Thanks to its independent assurance, the entire control and risk management system reaches the level of implementation necessary to ensure that the company's objectives are met and that the system works properly.

Furthermore, it emerges from the definition given by the IIA that internal auditors not only are independent, but they also result to be experts. Indeed, according to the definition of the word "assurance" that identifies an opinion/judgement expressed with a great level of conviction by a well informed and expert person in relation to a specific aspect, internal auditors need to have the right knowledge and expertise to ensure that their suggestions and opinions can really be considered worth of notice. Indeed, helping people to better execute their activities and to take the most suitable decisions for the entity and the control system, internal auditors need to continuously learn and develop the knowledge needed to assess and provide solutions to people who for long time have worked in a specific function and have a great level of expertise.

The Internal Audit function has to provide assurance on every aspect, process and mechanism of the organization, ensuring that the governance, control system and risk management result effective and efficient and appropriate to reach the strategic objectives of the entity.

According to what stated by IIA (2013), to allow the internal audit function to work as intended and to provide the expected outputs, some guidelines and best practices have been defined:

- Follow international standards in exercising the activities to it attributed;
- Ensure independence in the execution of its responsibilities through the reporting to high level functions in the organization;
- Develop direct periodic report to the entity's board to show results and any other issue emerging from the assessments conducted and present the audit plan for the following year.

The main responsibilities of the internal audit function are (Banca D'Italia, Circ. 285):

- Assess, also through the use of activities executed on site, the operating activities of the organization, and the evolution of risk and the relative actions used to contain it;
- Assess the adequacy of the governance in place and of the SCIGR, providing the Board with particular solutions to improve the system;
- Assess the efficacy of the RAF definition process;
- Execute specific audit activities, also on request of the Audit Committee, of the CEO or of the Supervisory Board;
- Present to the BoD the audit plan prepared by the Chief Audit Executive (CAE). This risk based audit plan is created through a process of analysis and prioritization of the principal risks and becomes binding once that it is approved by the Board. This plan represents the instrument used by the internal audit to continuously assess the activity and the appropriateness of the SCIGR (Quaderni Assirevi, 2016);
- Communicate periodically with the BoD to inform it about the results of the activities executed, the appropriateness of the SCIGR, and the respect of the Audit plan previously defined;
- Inform the Board of the emergence, identified during the execution of the audit activities, of specific issues and provide the Board with possible solutions.

While above are identified the main responsibilities of the internal audit function in the SCIGR, in chapter 3 will be described in detail the role of this function in risk management through the definition of those specific activities (provided by the COSO) that are within its duties.

In conclusion, as can be now easily understood, the Three Lines of Defense Model involves the participation of the three groups of actors described above. Each one of them results fundamental for the good result of the system.

Risk owners are the ones better knowing the business and the issues arising from it. They are the most appropriate to identify risks, assess them, mitigate them and then monitor them.

Risk managers are needed to ensure coordination among the actions undertaken by the different risk owners. Their intervention is fundamental to train and guide risk owners in the execution of

their duties and to let them contribute to the respect of the risk limits attributed to the function and of the general risk appetite set for the organization.

Finally, internal auditors are fundamental to ensure that the system receives independent and objective assessments to guarantee that the control and risk management system is implemented properly and that the strategic objectives are met.

Conclusion

As emerged from this chapter, the subjects involved in risk governance are numerous and each one responds and is accountable for the responsibilities to him attributed. Their expertise and their contribution are fundamental for the good output of the system. However, what results more fundamental is to ensure that coordination and communication mechanisms are in place to allow these subjects to share information and dispose of all the data needed to exercise their activities and facilitate the organization in exploiting the opportunities arising and reaching the objectives set in the strategic plan.

3. Research on the role of Internal Audit in Risk Management & on the coordination of the actors involved in risk governance

3.1 Independence of the IA function

In the previous chapter has been identified and described the group of subjects who participate to risk governance. The figures of internal auditors and risk managers and their related responsibilities have been illustrated while explaining the Three Line of Defense Model. These two functions are both fundamental within an organization to ensure that a proper control and risk management system is implemented.
As already emerged from the previous chapter, the responsibilities these two lines of defense have are different. The risk management function has to coordinate and provide guidance to all risk owners and to ensure that risks are addressed properly and are maintained within the risk appetite. Instead, the internal audit function has to provide an independent and objective assurance over processes and controls.

The aim of this chapter is to analyze more in detail the role of internal audit in risk management and the specific activities that, according to the new regulation and best practices, should be performed by one function or the other. Furthermore, are investigated also the coordination mechanisms instituted between the actors involved in risk governance. For the first scope of the chapter, great reference is done to the Position Paper produced in 2004 by the Institute of Internal Auditors called “The Role of Internal Auditing in Enterprise-wide Risk Management” about the role IA should have in ERM and the activities that are competence of each function.

Before proceeding with this analysis, there is the need to highlight that it is not possible to make a general statement on the responsibilities and duties strictly attributed to the second or the third line. As always emerged in this thesis, every organization has specific characteristics and governance systems and every entity shows a different level of maturity in their controls.
Before that the ERM concept started to gain the relevance it has nowadays, in providing its assurance over the processes of the entity, the internal audit function was also addressing the risk

owners to properly manage risks faced in order to ensure the good proceeding of the organization's activities.

However, as well explained in chapter 2, being fundamental to guarantee independence to the internal audit and objectivity to its assurance, regulators created principles, and associations (as the IIA) developed models that entities started to implement to enhance the independence of the function. Therefore, companies are slowly (changing the governance system and the structure of a company is not a fast process) modelling their control systems to ensure the presence of the different lines of defense with their related activities, but the level of implementation and appropriateness differs for every entity.

According to the Position Paper "The Three Lines of Defense in Effective Risk Management and Internal Control" issued by the IIA (2013), risk and control responsibilities should be assigned to different actors within the organization, which result to be accountable according to their roles. Furthermore, this paper states that if dual responsibilities are attributed to a single function or actor, entities should provide in a second time to divide them.

However, according to the Practice Guide issued by the IIA (2016), business constraints or additional issues might prevent the organization from applying this distinction in accountability. Examples of these constrains and issues are:

- The size of the organization is an indicator of the resources available for the company to implement independent control and assurance functions. Indeed, small organizations normally show less maturity in the implementation of the three lines of defense model;
- The internal audit has the competencies to execute risk management and compliance activities, and managers opt to attribute them these activities, rather than to the second line;
- Management or the BoD do not properly understand the relevance of maintaining a distinct and independent audit function that is able to provide objective assurance;
- Because of cost-cutting needs, internal audit decides to undertake second line's responsibilities and facilitates the company in this cost reduction;
- The maturity of the governance structure has an influence on the level of independence assured to the internal audit function.

Furthermore, it can be possible that even entities that already have in place a good risk management function or governance structure appoint the third line to perform second line activities. Reasons for this can be the following:

- New regulation and requirements: A new regulation, specially when entering in markets abroad, might require new and different efforts that would involve also the IA function;
- Resource constraints: Organizations might experience moments when economic resources result to be scarce or a change in staff might occur and the risk management function might experience difficulties in performing their ordinary activity;
- Efficiency: Managers or the BoD might decide that letting the IA perform second line of defense functions' activities would increase the efficiency of the corporate governance.

Therefore, before identifying the specific activities that the IIA suggests to attribute to the Second and Third Line of Defense, it is underlined that some companies might still make the internal audit function responsible for second line of defense functions as risk management and compliance. In this case, fundamental is to create protections to the independence of the IA and to its objectivity. In box 3.1 are identified some principles and elements to be applied related to the independence of the IA function and some safeguards that should be implemented when the internal audit has dual responsibilities.

Box 3.1: "*Internal Audit and the Second Line of Defense" (Practice Guide, IIA, 2016)*

When entities attribute to the IA second level functions and responsibilities, International Standards for the Professional Practice of Internal Auditing should be considered and applied within the organization to ensure the good result of the entire control system.

Following the main principles to be respected and implemented:

- **1100** Independence and objectivity
  The activity conducted by the internal audit has to be independent and the actors involved in this function need to be objective while making their job.

- **1110** Organizational Independence

  The Chief Audit Executive (CAE) needs to report to a level in the entity that allows its function to act independently. The IA function should not be involved in the management structure as the actors involved in the second line of defense who report to organizational management. Indeed, even in the case where second line functions are attributed to it, internal audit needs to maintain its independence reporting only to the BoD.

- **1120** Individual objectivity

  It should not only be created mechanisms and structures within the company that ensure autonomy of the internal auditors, but it is also extremely important to choose the right people for this function. Indeed, internal auditors need to have an unbiased attitude that prevent them from having and creating any conflict of interest.

- **1130** Impairment to Independence or Objectivity

  In case that the independence or the objectivity requirements (Standards above) are not met, timely communication should be provided to the right person.

- **2100** Nature of work

  The scope of the IA activity is to assess and participate to the improvement of risk management, governance and control processes.

Additionally to these standards, organizations attributing to the third line of defense also second line of defense functions should create safeguards to guarantee that independence is not compromised.

Following is a list containing examples of possible safeguards to be undertaken:

- Managers accept and become owners of risks;
- Roles are defined and assigned for each activity where the second and the third line of defense overlap;
- Evaluation is conducted on a periodic base by management and BoD to assess the reporting lines;
- Evaluation is conducted on a periodic base to assess the responsibilities assumed by the IA function in playing the second line of defense role and the level of independence and objectivity maintained by this function.

In conclusion, it is not possible to generalize on the governance structure of an organization and, even if it is well understood the relevance that an independent audit function has, various constraints might prevent entities from developing a control system based on three line of defense.

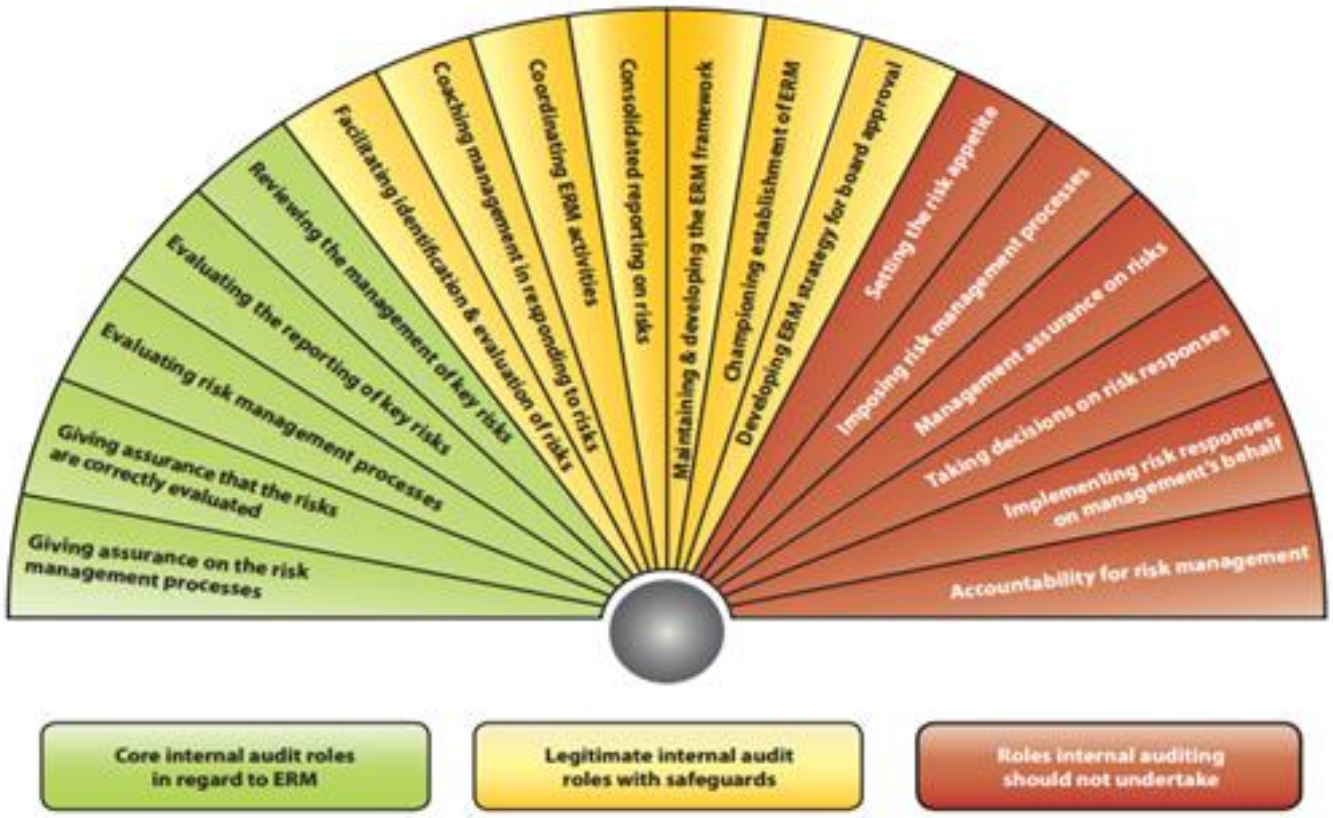
Bearing in mind what stated above, it is now possible to start with the analysis and description of the activities performed by the risk management and by the internal audit functions.

3.2 IA role in risk management

3.2.1 IA's role in risk management – fan of activities

As can be observed in figure 3.1, according to what stated by the IIA's Position Paper (2004), it is possible to categorize activities fundamental for risk management in 3 different groups. Starting from the left of the fan, the first range of activities identifies those actions representing the core roles of the IA, the second range represents activities that the IA might undertake but only with safeguards and the third range identifying those activities that should not be undertaken by the IA. The decision on how to group these activities is then conducted on the base of whether the specific activity undermines the independence and the objectivity of the internal audit function, and of whether the execution of this specific activity by internal auditors enhances the effectiveness of the risk management, governance and control system (IIA Position Paper, 2004). Therefore, it should be considered the benefit produced by letting the IA function execute these activities and, in case they would extremely increase the effectiveness of the risk management system but would reduce the independence of the IA function, it should be considered the trade-off between the two different effects produced. However, it is extremely important to remember that, for a proper execution of its role and responsibilities, the independence and objectivity of the internal audit function should be always considered as one of the most important aspects to bear in mind when attributing activities to internal auditors.

Figure 3.1: *Internal auditing's role in ERM*



Source: *IIA Position Paper: "The role of internal auditing in enterprise-wide risk management" (2009)*

Core IA roles in risk management

Each activity contained in the left range of the fan is an assurance activity.

To provide assurance is the most important way in which IA generates value for the company. Normally, the internal audit function provides assurance on three different aspects:

- Effectiveness of the risk management and internal control systems, including their layout and how well they are functioning to accomplish their aims and ensure that risks are addressed;
- Management of key risks faced by the company, involving also how promptly they have been identified and addressed, how effective are the systems and the actions put in place to control them and mitigate their effects and how they and their mitigation results have been reported;
- Appropriateness of the assessment conducted to identify and manage all risks faced by the entity, and of the reporting methods adopted to message risks and the mitigation results.

Therefore, as stated in the Standard 2120, "The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes".

A reasonable assurance cannot ensure that all risks or a specific one faced by the entity are maintained within an appropriate decided level. Instead, it can ensure that risk management, considered as a whole process running through the entire organization and considering aggregate enterprise metrics, is appropriate to achieve the organization's objectives and to let it meet its strategic plans.

Legitimate IA roles with safeguards

The center of the fan identifies those activities that are no longer part of the assurance area, but that instead extend into the consulting role of IA. Internal auditors might undertake these roles, but they have to ensure that safeguards are in place. Indeed, more we move to the right of the fan, more the internal audit independence will be threatened and greater will be the need for safeguards.

As already said, internal auditors are expert who acquired a wide knowledge on different areas being able to help the owner of risk in his role. However, even being able to do it, would it be appropriate?

The IIA (2004) has identified these legitimate IA roles with safeguards (identified and listed in box 3.1). They represent borderline roles that the IA could undertake being always careful in protecting the objectivity and independence of its function.

Looking at the center of the fan in figure 3.1 and bearing in mind the explanation of the Three Lines of Defense Model provided in chapter 2, it can be easily understood that roles as "facilitating identification and evaluation of risks" and "coaching management in responding to risks" are roles that risk managers should undertake in helping the first line of defense in executing their responsibilities. Again, activities as "Co-ordinating ERM activities", "Maintaining and developing the ERM framework", and "Championing establishment of ERM" should be performed by the risk management function that is the "coordinator" of the entire risk management system.

Being the assurance the main way in which the IA provides value to the organization, if internal auditors undertake these additional roles, they would lose their independence and reduce the quality of their assurance. Therefore, the only way in which IA would be able to preserve its independence would be through the adoption of safeguards and through the guarantee that

internal auditors would not assume any management responsibility and would provide only consulting services.

Some of the consulting roles that the IA might undertake related to the center of the fan's activities are (IIA, 2004):

- Provide management with tools, mechanisms and techniques used by the IA to assess risks;
- Provide guidelines and advises to risk managers and to the entire organization to develop a common understanding of risks and control and ensure a proper level of buy-in to the ERM;
- Provide support to managers in the identification of the best way to deal with risks.

In each of the points above, the IA provides consulting services to the actors involved in the risk management and control system without directly operate together with managers at those points. Indeed, managers will be the only one to decide whether or not, or how to put in practice the advice provided by internal auditors.

Roles IA should not undertake

Internal auditors should not undertake these six roles identified by the IIA (2004) because they represent a real threat to their independence and objectivity. Indeed, they would obligatorily and actively involve them in risk management, making them assume management responsibilities.

3.2.2 Risk Based Internal Audit

As also stated by the Chartered Institute of Internal Auditors ("Risk Based Internal Auditing", 2014), risk management and internal audit should be independent but at the same time should cooperate, and organizations should develop a Risk Based Internal Audit (RBIA). This latter is a mechanism that relates the IA activities to the risk management framework applied to the entire organization.

The implementation of this mechanism increases the focus given by the internal audit to risk management and the attention provided in the audit plan to this topic. As stated by the Chartered Institute of Internal Auditors ("Production of the audit plan", 2014), "RBIA is not about auditing

risks but about auditing the management of risk". It assesses how managers address specific risks, but also the general risk management process.

The continuous operation of the RBIA runs through three different steps (CIIA, 2014):

- Assessing risk maturity: Observing how managers and the board identify, assess, manage and monitor risks, internal auditors develop a first understanding and evaluation of the accuracy of the risk register. This preliminary information represents an initial guide for the IA when developing the audit plan for the following period.
- Periodic audit planning: On the base of the preliminary information gathered, are set the assurance and consulting activities for the following period. The definition of these assignments is influenced also by the needs of and by the activities required by the BoD, its Audit Committee and the Director of the SCIGR.
- Individual audit assignments: On the base of the plan previously produced, individual audit activities are assigned and assurance is provided on the risk management system, and the way in which it operates in the identification, assessment, management and monitoring of risks.

A wider description of Risk Based Internal Audit is provided in box 3.2. The different stages and their relative objectives are shown so that it is better understood the relation between risk management and internal audit and the huge focus that the internal audit plans and activities have on risk management.

Box 3.2: *"Risk Based Internal Audit", Chartered Institute of Internal Auditors (2014)*

Risk maturity assessment

The three objectives of the risk maturity assessment (that is the first step of RBIA) are:

- Make an evaluation of the risk maturity of the entity;
- Report the results of this assessment to the management, to the BoD and to the audit committee;
- Decide, together with the actors identified in the point above, the audit strategy.

To reach these objectives, the activities that the internal audit function has to perform are various.
Firstly, they have to conduct an assessment to understand what has already been executed to enhance the risk maturity of the entity. This activity is meant also to identify whether risk managers understand risk management and the responsibilities they have not only in the identification, measurement and mitigation

of risk, but also in the continuous monitoring of risks, mitigation actions in place and the framework.

This action helps to identify also whether managers are comfortable with the risk register created and whether they believe that it is comprehensive.

Secondly, internal auditors should gather additional information through specific documents that should be provided to them. Indeed, it is not sufficient to assess the understanding of risk maturity that the management and the board has to determinate the level of risk maturity of the entity. Therefore, documents containing information regarding the organization's objectives, the way in which risks are identified and analyzed, the definition of the risk appetite, the way in which risk is taken into account during decision-making activities, the commitment to risk management and the entity's risk register are needed to produce a much more accurate assessment of the risk maturity. Furthermore, any previous assessment conducted by the management or the board in relation to the risk maturity of the entity would work as starting point for the internal audit activity.

Once that the internal audit has conducted its preliminary assessment and that the additional information have been provided by the management, internal auditors are ready to make their assessment on the level of risk maturity of the entity.

The conclusions made represent a first level of assurance on the risk management process, its phases and the commitment of managers to this system. These conclusions are reported to the audit committee and to managers.

Finally, the fifth and the sixth actions involve the definition of the audit strategy and its components. Working and interacting with the management, managers might suggest some actions that the IA might execute to provide advices and assurance on specific aspects. On the base of the result of all the previous activities, the internal audit function decides its strategy and reports it to the approval of the management and the audit committee.

The audit strategy normally includes three potential elements:

- The assurance that internal auditors plan to provide;
- The framework on which will be based the entire audit plan (organizations having a well developed risk register will let the assurance of IA focus on it);
- The consulting services and advices that internal auditors plan to give (less risk mature organizations will need more advices on how to enhance their risk maturity).

It is important to underline that the nature of the advice is agreed with the costumers and that the consulting activity performed by internal auditors never attributes them management responsibilities.

Production of the audit plan

The objectives of the production of the audit plan (that is the second step of the RBIA) are:

- Decide all the risk management processes and specific mitigation actions on which is needed the assurance provided by the internal audit function;
- Once that these elements are decided, create an audit plan including and identifying all audits that need to be conducted over a defined time range (normally a year).

To reach these objectives, the activities that the internal audit function has to perform are various.

Firstly, internal auditors should analyze all the documents, including the risk register, obtained during the first stage of the RBIA. Furthermore, they should consider the assurance requirement obtained by the audit committee and the management. These requirements represent the specific needs of assurance that these actors have, and they represent a guidance for the IA in setting the audit activities. However, in setting these activities, internal auditors might opt to give assurance only on some identified aspects of the risk management framework. Effectiveness is not necessarily enhanced through an overall assessment of the system; indeed, it might be more effective to focus the efforts on those aspects and risks that mostly need assurance.

Therefore, the second activity performed to create the audit plan is to categorize and prioritize risks. They might be categorized according to the business unit, the function or system, or the objectives the organization has.

The responses to risks should also be categorized and prioritized. They might be categorized according to:

- The size of the risk mitigated (greater is the risk, greater is the exposure and the potential negative effect for the organization, and greater is the need for assurance);
- The effect of the mitigation on the exposure (greater is the effect of the mitigation in place, and greater becomes the need for assurance);
- The number of other assurances already provided on the effectiveness of the mitigation (greater is the assurance already available, and lower is the need for further assurance).

Once that also this activity is executed, the internal audit function is now able to assign risks to audit activities and to start to design the audit plan. In designing and creating the audit plan, it is considered the time needed for each audit activity and it is identified whether the available resources are sufficient to execute these activities or if additional ones are needed.

Finally, this plan is discussed with the Board and the audit committee for approval. The Board and the audit committee should be informed of any assurance by them required that will not be executed by the IA.

Doing the audit

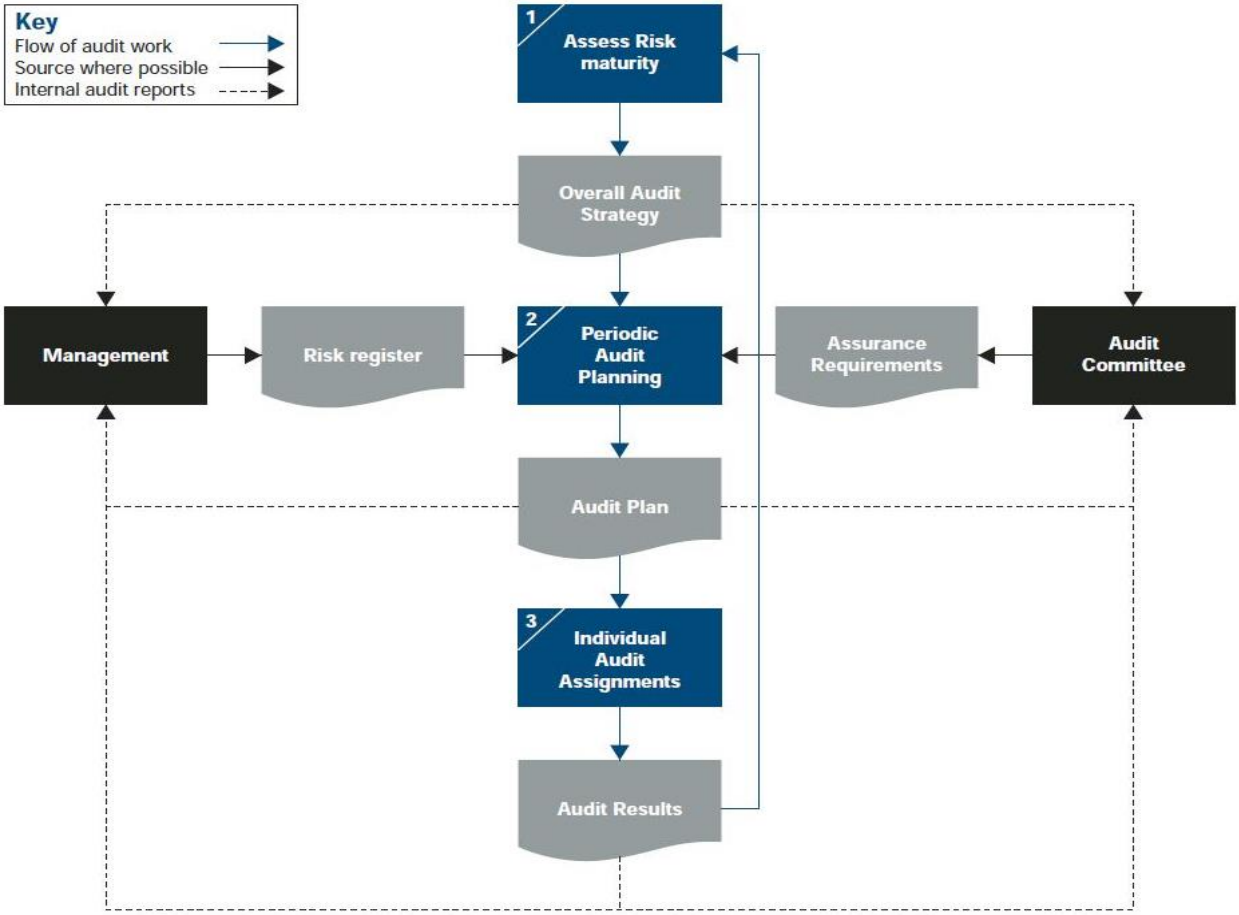
The objective of doing the audit (that is the third stage of the RBIA) is to provide assurance that:

- Managers have identified, measured and responded to risks;
- Mitigation actions are implemented and result not to be excessive in containing risks addressed within the risk appetite;
- Actions are taken when residual risks are still too high, resulting to be over the risk appetite;
- Risk management system is monitored and the process continuous to be effective.

To reach this objective, the activities that the internal audit function has to perform are various.
Firstly, internal auditors have to define the scope of the activity to be conducted. On the base of the information gathered in the first and second stages, they have to design the draft scope.
Secondly, internal auditors conduct a deeper assessment than the one made in stage 1 and set the risk maturity of the specific business or department analyzed. During this further assessment, the criteria used should be consistent with the ones used in the assessment conducted in the first stage.
If the actual risk maturity results to be higher or equal to the maturity expected from the first stage, then it is possible to continue with the assessment of the mitigation actions undertaken. If the actual maturity is instead lower, internal auditors should inform the management about it and about the fact that the mitigation actions undertaken (part of the audit scope) might not be appropriate.
Then, internal auditors assess that the control systems used by management are appropriate to ensure that the organization reaches its objectives. Furthermore, they assess that the actions in place are appropriate and that the right level of attention to risk is given.
Once that these analysis are conducted, internal auditors document their activities and create reports including also conclusions and possible suggestions. Finally, the audit conclusions are summarized to be presented to the audit committee and to the BoD.

As described in the previous pages and as is shown in the figure 3.2, internal auditors should not be directly involved in the risk management activities. They should instead interact with all the other actors involved in the risk management and control system, ensuring that their actions are reliable and that the system on the overall is properly working.

Figure 3.2: *Stages of the RBIA*



Source: *IIA "Risk based internal auditing" (2015)*

3.3 Research on the IA role in risk management

3.3.1 Introduction

In this chapter has been widely described, through the reporting of best practices and principles, the role that the internal audit function should have in managing risk. However, as also highlighted at the beginning of the chapter, the fan of roles identifying those roles that the IA should or should not undertake appear to be a guideline that not necessarily is followed by organizations and then that not necessarily reflect the reality for each entity. Therefore, this chapter wants to make a step further than simply investigate the theoretical roles that the internal audit could undertake, and it wants to observe the actual situation declared by Italian listed companies.

A research has been conducted to assess the roles that the internal audit function of the thirty companies already analyzed in chapter 1 have undertaken. This research is based on the Corporate Governance reports issued by these entities. As already explained in chapter 1, these reports are official documents that follow specific principles and accomplish to specific governance requirements of the Italian listed companies rules or of the Codice di Autodisciplina (hereinafter "the Code"). Therefore, it has been chosen this methodology to ensure that data reported are accurate and certified.

However, before starting with the research, it is important to highlight again that results are based only on what has been reported by entities and that this study is a scrupulous analysis of these declarations.

3.3.2 Research development

This research has been meant to identify if the fan of roles (providing assurance or consulting services) presented in paragraph 3.2.1 actually reflects the roles that the IA function of the thirty Italian listed companies already assessed above have undertaken.

To reach this objective, it has been observed the declaration produced by each of these organizations in relation to the audit activities conducted during 2015 and in relation to the responsibilities that this function generally has. The decision to base the analysis on these two aspects has been led by the fact that the majority of the organizations seems to formally comply with the requirements of "the Code", scrupulously reporting the roles and responsibilities identified in the art. 7.C.5 (of "the Code").

It is believed that an analysis that considers also the activities conducted by the internal audit function during 2015 (when available) would produce a much more accurate representation of the roles actually undertaken.

The fan of activities identified in paragraph 3.2.1 has been used as key element to assess the reports. Indeed, this study tried to analyze and recognize which of the roles included in the fan were actually undertaken while performing specific activities, and to classify the internal audit activity as "assurance" or "consulting services" or "risk management role".

Below is presented a table (table 3.1) containing for each company two important types of information contained in two different columns.

The first column after the company name shows specific activities that the entity reported in the Corporate Governance report and that have a particular relevance when assessing the role that the internal audit has in managing risk. In presenting these activities, great attention has been payed to reconnect them with the fan of activities and to scrupulously understand what companies have declared even if shortly mentioned.

The second columns defines instead, on the base of what reported in the previous column, if the internal audit function has provided assurance (left side of the fan) and/or advices (central part of the fan) and/or has performed activities that are normally competence of the risk management function.

Table 3.1: *IA's role in risk management in the 30 Italian listed companies' sample*

Company	Actions/roles	Role's category
ENI	The IA function assures that the SCIGR and all its processes properly work. It assures that risks are properly managed and that their mitigation actions are correctly put in practice (periodic monitoring). The audit plan is a risk-based plan created following a top-down approach to risk. Furthermore, the IA provides consulting services to top management and to management through advices on how to enhance the risk and control systems (also on how to respond to risks).	**Assurance, Consulting** (safeguards to ensure independence of IA)
ENEL	The IA function assures that the SCIGR and all its processes properly work. It assures that risks are properly managed and that their mitigation actions are correctly put in practice (periodic monitoring). The audit plan is a risk-based plan.	**Assurance**
Intesa San Paolo	The IA function assures that the SCIGR and all its processes properly work. It assures that risks are properly managed and that their mitigation actions are correctly put in practice (periodic monitoring). It produces a risk assessment to identify the emergence of new relevant risks and to structure the IA plan over these findings. Furthermore, it provides advice on how to improve the RAF, the risk management system and the assessment and the mitigation of risks.	**Assurance, Consulting** (safeguards to ensure independence of IA)
Luxottica Group	The IA function assures that the SCIGR and all its processes properly work. In the CGR, it is not evident the focus on risk of the internal audit activities.	**Assurance**

Generali	The IA function assures that the SCIGR and all its processes properly work. It assures that risks are properly identified, measured and managed and that their mitigation actions are correctly put in practice (periodic monitoring). It provides assurance on the activities of the 2nd line. The audit plan is a risk-based plan. Furthermore, the IA provides consulting services in the mitigation of risks and in the control and risk management processes.	**Assurance, Consulting** (safeguards to ensure independence of IA)
Atlantia	The IA function assures that the SCIGR and all its processes properly work. It assures that risks are properly identified, measured and managed and that their mitigation actions are correctly put in practice (periodic monitoring). It provides assurance on the activities of the 1st and 2nd line. The audit plan is a risk-based plan. Furthermore, the IA provides consulting services to management through advices on how to enhance the risk and control systems.	**Assurance, Consulting** (safeguards to ensure independence of IA)
UniCredit	The IA function assures that the SCIGR and all its processes properly work. The audit plan is created on the base of the results of the Risk Assessment and it ensures that the key risks are properly managed and their mitigation actions are properly undertaken. Risks are evaluated and new risks emerged by the assessment are promptly communicated. Furthermore, the IA function provides advices on how to design, implement, and enhance the control and risk management system.	**Assurance, Consulting** (safeguards to ensure independence of IA)
SNAM	The IA function assures that the SCIGR and all its processes properly work. It evaluates risk management and assures that risks are properly addressed. The audit plan is based on a process of prioritization of the principal risks made by the ERM function. Mainly formal compliance with the Code.	**Assurance**
Tenaris	**Not described in the report.**	
Telecom Italia	The IA function assures that the SCIGR and all its processes properly work. It evaluates risk management and assures that risks are properly addressed. The audit plan is a risk-based plan. It declares to provide also advices (without specifying if they are provided to risk management activities). Mainly formal compliance with the Code.	**Assurance**
Terna	The IA function assures that the SCIGR and all its processes properly work. It evaluates risk management and assures that risks are properly addressed. The audit plan is a risk-based plan. The "Full External Quality Assessment" has certified that the internal audit activity is directed to contribute to risk management (also through consulting services). Mainly formal compliance with the Code, with the exception of the recognition provided by the Full External Quality Assessment".	**Assurance, Consulting** (safeguards to ensure independence of IA)
CNH Industrial	**Not described in the report.**	

Poste Italiane	The IA function assures that the SCIGR and all its processes properly work. It evaluates risk management, assures that risks are properly addressed and that the mitigation actions identified are properly implemented. The audit plan is a risk-based plan. The IA function provides also advices to management to ensure the enhancement of control and risk management processes. Two IA functions exist in the company.	**Assurance, Consulting** (safeguards to ensure independence of IA)
EXOR	The IA function assures that the SCIGR and all its processes properly work. It evaluates risk management and assures that risks are properly addressed. The audit plan is based on a process of prioritization of the principal risks. Mainly formal compliance with the Code.	**Assurance**
FCA	The Global Internal Audit function defines its audit plan on the base of the results of the Risk Assessment. Audit activities are planned for global enterprise risk management ("ERM") significant risks. In the 3 lines of defense model, the 3rd line is covered by Enterprise Risk Management functions.	**Assurance**
Recordati	The IA function assures that the SCIGR and all its processes properly work. It assures that risks are properly managed and that their mitigation actions are correctly put in practice (periodic monitoring). Furthermore, the IA function helps the director of the SCIGR in the creation, management and monitoring of the ERM framework, and in the identification of risks.	**Assurance, Consulting** (safeguards to ensure independence of IA)
Parmalat	Missing the 2nd line of defense, the IA function not only provides assurance as required by the Code (7.C.5), but it also directly identifies and contains risks. Parmalat declares that the IA function is independent in terms of organizational report, but this function performs also risk management activities (right side of the fan's roles).	**Assurance, Consulting, Risk management roles**
HERA	The IA function assures that the SCIGR and all its processes properly work ensuring that the risk exposure stays within the risk appetite. It evaluates the main risks and how they are identified and contained. The audit plan is based on a process of prioritization of the principal risks identified. The IA conducts a risk assessment.	**Assurance**
De' Longhi	The IA function assures that the SCIGR and all its processes properly work ensuring that the risk exposure stays within the risk appetite. It evaluates the main risks and how they are identified and contained. The audit plan is based on a process of prioritization of the principal risks identified. The IA conducts a risk assessment. Furthermore, the IA function helps the director of the SCIGR in the creation, management and monitoring of the ERM framework, and in the identification of risks. During 2015, the IA continued to work at the risk management project finalized at strengthening risk management.	**Assurance, Consulting** (safeguards to ensure independence of IA)

Brembo	The IA function assures that the SCIGR and all its processes properly work. It assures that risks are properly managed and that their mitigation actions are correctly put in practice (periodic monitoring). Furthermore, the IA provides consulting services to management through advices on how to enhance the risk and control systems.	**Assurance, Consulting** (safeguards to ensure independence of IA)
Diasorin	The IA function assures that the SCIGR and all its processes properly work. It evaluates risk management and assures that risks are properly addressed. The audit plan is based on a process of prioritization of the principal risks. Mainly formal compliance with the Code.	**Assurance**
ACEA	The IA function assures that the SCIGR and all its processes properly work. It assures that risks are properly managed and that their mitigation actions are correctly put in practice (periodic monitoring). Furthermore, it provides consulting services to management and top management for the identification and evaluation of the main risks.	**Assurance, Consulting** (safeguards to ensure independence of IA)
Banca Generali	The IA function assures that the SCIGR and all its processes properly work. It evaluates risk management and assures that risks are properly addressed. Furthermore, the IA provides consulting services to management through advices on how to enhance the risk and control systems, the Risk Appetite Framework and on how to measure and control risks.	**Assurance, Consulting** (safeguards to ensure independence of IA)
Inwit	The IA function assures that the SCIGR and all its processes properly work. It evaluates risk management and assures that risks are properly addressed. The audit plan is a risk-based plan. It declares to provide also advices (without specifying if they are provided to risk management activities). Mainly formal compliance with the Code.	**Assurance, Consulting** (safeguards to ensure independence of IA)
IMA	The IA function assures that the SCIGR and all its processes properly work. It assures that risks are properly managed and that their mitigation actions are correctly put in practice. The Chief Auditor Executive (CAE) is **not independent**, being responsible of the Quality and Compliance function and reporting (for this role) to the General Services Direction.	**Assurance** (not independent)
Credito Emiliano	The IA function assures that the SCIGR and all its processes properly work. It assures that risks are properly managed and that their mitigation actions are correctly put in practice. The audit plan is a risk-based plan. Mainly formal compliance with the Code.	**Assurance**
Ansaldo	The IA function assures that the SCIGR and all its processes properly work. It assures that risks are properly managed and that their mitigation actions are correctly put in practice. The audit plan is a risk-based plan. Mainly formal compliance with the Code.	**Assurance**

SIAS	The IA function assures that the SCIGR and all its processes properly work. It assures that risks are properly managed and that their mitigation actions are correctly put in practice. The audit plan is created on the base of the results of the Risk Assessment (conducted by the entity) and of the additional information related to the main risks.	**Assurance**
Amplifon	The IA function assures that the SCIGR and all its processes properly work. It assures that risks are properly managed and that their mitigation actions are correctly put in practice. The audit plan is created on the base of the results of the Risk Assessment (conducted by the entity), of the additional information related to the main risks. Furthermore, the IA function facilitates the identification, assessment and management of company's risks.	**Assurance, Consulting** (safeguards to ensure independence of IA)
Autogrill	The IA function assures that the SCIGR and all its processes properly work. It assures that risks are properly managed and that their mitigation actions are correctly put in practice. The IA assesses how risks are identified and evaluated in coherence with the ERM model adopted by the Group.	**Assurance**

3.3.3 Comments on the research

The research developed above investigated which are the actual roles in the management of risks that the internal audit function of the sample of entities undertakes, and how these roles are classified, considering the fan of roles, between "Assurance", "Consulting" and "Roles that should be undertaken by the risk management".
Before proceeding with the analysis and comments on the research, it is furtherly stated that the considerations that will follow are entirely based on the Corporate Governance Reports. Therefore, judgments and specific assessments on the IA function of the organizations will not be contained in this study because companies might have faced some formal deficiencies in creating the report that are not actually reflected in the reality of the company.

The first evidence arising by table 3.1 above is that almost all entities "formally" comply with what required by "the Code" (7.C.5), reporting in their reports the exact Criteria so as it is written in the Code. Great attention has been paid to assess and understand which company was only formally complying and which instead was enlarging what explicitly required with some personal characteristics. In table 3.1 have been identified with a green sentence those organizations that were mainly formally responding to the code.

Those companies that went deeper than what explicitly required by "the Code" in reporting information are also the same that rank higher in terms of market capitalization (companies in the table are ranked on the base of the mkt cap, starting from the biggest one). However, before proceeding with a deeper assessment of these entities, it is important to focus still a bit on the role undertaken by the IA function of those companies that at least formally comply with "the Code". The Criteria 7.C.5 identifies (through its lett. a-h) mainly an assurance role for this function. Therefore, when observing the results for these entities it is not a surprise that all their roles are classified as "Assurance", and that they all assure that the SCIGR and its processes are properly working and that risks are properly identified, assessed and addressed. Furthermore, they all report that the IA's plan is risk-based.

Another interesting thing to note is that 2 companies, Tenaris and CNH Industrial, being subject to a different authority and being listed also in other markets, do not have to necessarily disclose information about the Internal Audit function. For this reason, information in the table above are missing for these 2 organizations.

A further consideration is that rarely (only one case, Parmalat) the IA function undertakes roles that should be attributed to the risk management function, but instead it is not so rare that it provides consulting services. Indeed, exactly the **50%** of the sample provides these services. This percentage is important if it is considered that in the last decades the definition of the IA's role and responsibilities has been modified to include also the consulting role. Therefore, even if this percentage is not low, it seems not to entirely capture this enlargement in the roles.
During the analysis of the sample above, it emerged that 2 main kinds of advise are produced by internal auditors. The first one is related to the enhancement of the control and risk management system (overall advise on the process), while instead the second one is related to the enhancement of the risk identification, measuring, mitigation and monitoring through a direct help provided to management and top management. In the Corporate Governance Report of these organizations whose IA offers consulting services it is declared that safeguards are put in place and that the independence of internal auditors is ensured.

Regarding the only case where the IA function seems to undertake roles that should be of competence of the risk management function, looking at table 1.2 (chapter 1) it is possible to

observe that Parmalat is one of the companies that scored the worst in the assessment of the implementation of the ERM system. Indeed, in the Corporate Governance Report of this company, rather than describing the Three Line of Defense model implemented, it is described a two line of defense where the first line is composed by the risk owners and the second line is covered by the internal audit. Therefore, missing the second line of defense it appears inevitable that the IA function results to assume risk management roles, i.e. in directly identify and mitigate risks.

Additional considerations that arise from the study are the following:

- Luxottica Group appears to be the only one that makes no explicit reference to risk management and that generates an audit plan not considering the main risks emerged. Therefore, the Risk Based Internal Audit seems to be missing in the firm's declarations.
- FCA has implemented a particular governance structure. The third line of defense is composed by Enterprise Risk Management functions and little description is provided in relation to the role the internal audit has. As has been shown in table 1.2 (chapter 1), FCA has been one of those companies that more creatively have implemented a proper enterprise risk management system.
- The CAE of IMA results to be not independent. Indeed, being responsible of the Quality and Compliance function, he reports (for this role) to the General Services Direction.

Finally, the **20%** of the entities in the sample seem not only to formally comply with what required by the code, but also to enlarge the description with specific characteristics of the roles and responsibilities of their 3rd line of defense. These entities are ENI, Intesa San Paolo, Generali, Atlantia, Unicredit, De' Longhi. Looking at these companies, the first consideration that can be conducted is that bigger is the company (in terms of market capitalization) and greater will be the availability of resources to create and implement a proper IA function. Moreover, bigger the organization and greater the need to ensure that risks are properly addressed and that the achievement of the strategic objectives is not undermined.
The second consideration that can be done is that the **50%** of the entities included in this smaller group are entities operating in the financial sector (banks and insurance). Therefore, comparing the 3 financial entities with ENI (oil & gas - utilities), Atlantia (industrial) and De Longhi' (consumer goods), it is evident that the financial sector is prevalent (50%) compared to the three other sectors that equally divide the remaining 50%.

3.4 Coordination between the actors involved in risk governance

As described in chapter 2 and further assessed previously in this chapter, the actors involved in risk governance are numerous and they all contribute to ensure that the control and risk management systems in place are appropriate to guarantee that the entity achieves its objectives. The new trends and needs in terms of corporate governance are directed to ensure an efficient and effective governance and control system. To satisfy these emerging needs, there is the necessity that all the subjects involved have a clear understanding of their roles and responsibilities, and that they cooperate in order to avoid duplicates in the work done and in the efforts made and to avoid wastes of resources.
According to what stated in the Practice Guide "Coordinating risk management and assurance" of the IIA (2012), many entities are organized in and dispose of different groups performing risk management, compliance and assurance activities independently from the others. However, without coordination between these groups, three main problems might arise: duplications, inconsistencies in controls and missed controls.

There is a wide range of literature available treating the coordination between the subjects involved in the governance. Institutions, organizations and regulators have identified the ways they believed to be the best to let the actors involved coordinate.

The Associazione Nazionale Direttori Amministrativi e Finanziari (ANDAF) has issued a guideline for the "Sistema di controllo interno per il governo dei rischi nelle PMI". In chapter 7 of this guideline, ANDAF identifies the coordination mechanisms between the control functions. This paper offers many practical proposals on how an entity may accomplish in this scope. Specifically, it lists the following actions:

- Create, develop and distribute shared methodologies, techniques, and evaluative instruments, tools and metrics. This action ensures alignment and coherence on how the different functions operate, make their evaluations and report the results of the activities performed.

- Define in a coordinate way the different roles and responsibilities attributed to the different functions, so that are avoided overlaps and uncovered activities. In the definition and attribution of these roles and responsibilities, it should be provided a systemic representation of the activities to be performed, including descriptions and details for the sublevels of every function.
- Continuously communicate on the monitoring executed and on the actions performed. The coordination is ensured by flows of information and, when needed, by the meeting between the management of the different function.
- Spread and share the risk assessment conducted by the risk management function and the relative risk map created to the other functions within the entity. This assessment could be the starting point of the activity performed by other actors and prevent them from re-executing an activity already performed, wasting additional resources.
- Define the control plan of every function in accordance to the plans of the others.

Assirevi, in its workbook about "L'esercizio del risk oversight da parte del CdA" (2016), underlines the importance of the information flows at every level of the organization. Furthermore, it defines some specific characteristics that this information should have. It should be complete and synthetic, accurate, comparable, traceable, and timely.

The Circ. 285 (2013) of Banca D'Italia containing the "Disposizioni di vigilanza per le banche" provides important directives in terms of coordination. The new requirement of the BI to ensure the correct integration of all the different functions, avoiding overlaps and gaps, is that the body responsible for strategic oversight (normally the BoD) approves a document containing relevant specific information.
In this document are indeed defined roles and responsibilities of the different actors involved, the information flows occurring between the different functions, and the coordination and collaboration mechanisms to be implemented in case in which the responsibilities distributed generates potential overlap or allows the creation of synergies.

Since now, it has been described the set of rules and the literature spectrum related to the forms of coordination between the subjects involved. However, also on observing this aspect, this thesis wants to make a step further than simply investigate the theoretical mechanisms that could be

used to ensure coordination, and it wants to observe the actual situation declared by Italian listed companies in their Corporate Governance Reports.

3.5 Research on the coordination between the actors involved in risk governance

3.5.1 Research development

Starting from this year, "the Code" has required entities to explicate in a specific paragraph of their Corporate Governance Reports the coordination mechanisms they implemented. Therefore, to understand how the different actors involved in the governance of the organization actually collaborate, attention has been payed to what declared in the part of the report accomplishing with the new requirements of the Code. However, before starting with the research, it is worthy to recall again that results are based only on what has been reported by entities and that this study is a scrupulous analysis of these declarations.

In table 3.2 below is assessed which kind of mechanism every entity has put in place. For simplicity and space reasons, in the head row are not shown the coordination mechanisms titles. Instead, in the head row are contained some alphabetic letters that correspond to specific mechanisms according to the matches below:

A – Spread of a common language

B – Adoption of common and shared evaluation methods and instruments

C – Creation of continuous information flows

D – Creation of institutional occasions in which functions can meet to coordinate

E – Definition of the roles and responsibilities attributed to each function

F – Creation of the document required by Banca D'Italia (described in paragraph 3.4)

Table 3.2: *Assessment of the coordination mechanisms*

Entity	A	B	C	D	E	F	Notes
ENI							
ENEL			x				2nd line refers to the 3rd the issues to be assessed and the 3rd communicate results to the parts involeved.
Intesa San	x	x	x	x			

Paolo							
Luxottica Group							
Generali							
Atlantia			x				Coordination of the information flow is assigned to the CEO.
Unicredit		x	x	x	x	x	Creation of the "Documento degli Organi Aziendali e delle Funzioni di Controllo" required by BI. Managers can share information during the managerial committee dedicated to control topics. Very good also the coordination between 2nd and 3rd line of defense.
Snam							
Tenaris							
Telecom Italia					x		The paragraph assessed reports a clear definition of all the roles and responsibilities attributed to each function.
Terna			x	x	x		Widely described roles and responsibilities attributed to each function, and all the flows and meeting occasions that are put in place.
Poste Italiane	x	x	x	x			Impressing the attention Poste pays to report all the different information flows.
CNH Industrial							
Exor					x		It is declared that roles are analytically assigned
FCA							
Recordati				X	x		Widely described all the occasions when the subjects meet. It seems to focus more on these specific situations rather than on a continuous flow of information.
Parmalat							
Hera			x	x			Widely described all the occasions when the subjects meet. Creation of a risk committee that provides guidance on the strategy to follow in dealing with risks.
De' Longhi			x		x		Widely described all roles and responsibilities attributed to the different functions.
Brembo			x	x	x		Identified the roles and responsibilities assigned to some specific functions and is described how, in explicating these duties, the function reports to and communicate with other ones.
Diasorin			x				Coordination of the information and of the parts involved is assigned to the CEO.
Acea			x	x			
Banca Generali			x	x	x		Described the presence of specific meetings where managers coordinate and of information flows (through reporting). Roles and responsibilities are identified.
Inwit					x		
Ima				x			
Credito Emiliano	x	x	x		x	x	Creation of the "Documento degli Organi Aziendali e delle Funzioni di Controllo" required by BI.
Ansaldo STS			x		x		Described the roles involved.
SIAS				x	x		Cited the reporting activities of the subjects involved.
Amplifon							
Autogrill					x		
Total	**3**	**4**	**14**	**11**	**13**	**2**	

3.5.2 Comments on the research

The first consideration that can be done on the results contained in the table above is that 21 out of the 30 organizations (equal to a **70%**) have complied with the Code and have reported in a dedicated paragraph the coordination mechanisms implemented within the entity. Even if not the entire sample has accomplished with the new requirements, the number of organizations that positively responded to the new request (even if sometimes they appear only to do it formally) can be considered satisfactory. Indeed, being it the first year in which entities had to explicitly provide this information, to obtain a number greater than the half of the companies of the sample shows that they are positively responding to the new requirements.
Furthermore, almost all the companies (13 out of 15) ranking in the second half of the sample in terms of market capitalization provided information about the coordination mechanisms. In this case, opposite to the results of the other studies previously conducted, the size of the organization has not led to the conclusion that bigger is the company and better the output of the analysis.

A conclusion that instead is aligned to those of the other studies is that the sector in which the company operates plays a role. From table 3.2 it is possible to evince that the organizations that scored the best, declaring all at least 4 out of the 6 mechanisms investigated, are those organizations operating in the financial sector. These entities comply with the regulation of their sector and for this reason they perform much better than the others. As it is well known, the financial sector is much more regulated than other ones and it is not a surprise that these entities better describe their coordination methods.
Moreover, 2 out of the **4** entities declare to have issued the document required by BI that contain all the information related to the coordination mechanisms implemented.

A different kind of consideration can be done in investigating which are the coordination methods that mostly recurred in the Corporate Governance Reports of the thirty entities.
There are two types of elements that scored the most. The first one is represented by the coordination ensured through a clear definition of roles and responsibilities that avoids gaps and overlaps. The second one is composed by mechanisms as information flows and institutional meetings/reporting that allow the coordination through sharing of results, data and information.

In relation to the first type, it has been observed that many entities of the sample have populated this additional paragraph created in the CGR with a summary of the roles and responsibilities of each function already explained before. These entities have made a first step toward the accurate declaration of all the coordination mechanisms in place, but they show the need to further explain how the subjects identified practically integrate and collaborate.

The second type is extremely popular in the declaration of the companies that accomplished to the new requirement. Indeed, even companies that poorly describe the coordination methods normally report that information flows occur within the entity. Moreover, some of these companies, rather than call the paragraph “coordination between the subjects involved” called it information flows.

Conclusions

In this thesis the aspects that have been investigated in the CGR of the thirty Italian listed companies are: the status of implementation of ERM, the role of IA in risk management and the coordination of the actors involved in risk governance.

As explained in the first chapter, risk management has assumed and continues to assume day after day more relevance in the management of companies. Indeed, entities became more aware that a well designed and implemented risk management function and the diffusion of a risk culture within the organization can ensure a better achievement of the strategic objectives set and a better chance to contain risks and exploit the opportunities arising by them. In this new environment risk management evolved and improved to be always able to match company's needs. Nowadays, the new best practice in terms of risk management is Enterprise Risk Management. As it has been observed, there is a wide range of literature explaining the elements of this process and the benefits for companies, and a wide number of directives and principles of regulators and institutional organizations. Considering all these aspects, it could be believed that this best practice is widely diffuse and implemented by companies. However, the results of this study are not aligned with the believe above.

Indeed, the majority of the companies assessed appear to be only formally compliant to the requirements of regulators reporting exactly what required to declare and failing to provide additional information of how they actually implement the aspects and the key elements of ERM. From the analysis conducted, it appears that companies are changing their control systems and are giving more importance to the risk management function, but it appears also that they still have to make efforts to properly implement what required. Furthermore, a formal compliance let arise doubts on what reported by companies. It appears indeed dubious that these organizations, even being different and having different governance structures, report exactly the same aspects when describing the SCIGR.

Another consideration is that there is evidence that some specific aspects of the entities played a big role in let them rank higher when assessing the risk management system.

The size of the organization in terms of market capitalization resulted to be an important element. 11 out of the 14 companies that scored above the threshold set for the aim of the study are part of the FTSE MIB basket. Bigger is the entity and greater is the available capital, and more mature will result the risk management system, being the company more able to invest to implement a better structure to manage and control risks. Furthermore, bigger and more complex is the company and greater will be the willingness and the need of the company it-self to develop a greater risk management system to manage all those events that would create deviations from expected and to let the company continue to perform well enhancing its value.

The macro-sector in which entities operate is another of the elements that this study discovered to influence the results obtained when assessing risk management systems. Indeed, some sectors are subject to a wider regulation that imposes them to comply with further requirements. In example, entities operating in the financial sector seem to have a more mature ERM.

The last aspect that has been discovered to influence the results obtained is the presence of the entity in foreign markets. Indeed, having to respond to different regulatory requirements and being listed in other stock exchanges, these entities have to comply with additional laws. Because of this aspect and because of the willingness of multinational companies (as ENI) to acquire the best practices in use in the different countries where they operate, these entities present a better implemented ERM system.

The general conclusion of the first research is then that ERM is surely perceived by regulators, authorities and entities as a best practice that, if well put in place, would increase the value of the organization. However, even if the benefits are clear, companies are still struggling (with some exceptions) to properly implement this system and they appear to comply mainly formally with what required by the regulator. This formal compliance that let the majority of the organizations report the same aspects let arise doubts on the goodness for the entities' statements implementation.

Finally, it has been observed that some specific entities' characteristics (size, sector of activity, geographic scope) are indicators of the success of a proper ERM implementation.

As it has been described in chapter 2, important elements of enterprise risk management are a risk culture spread within the organization and the participation of all entities' employees to risk management. Therefore, the actors involved in risk governance are numerous and the need of

coordination is high. Nowadays, entities are much more focused on ensuring the efficiency and the effectiveness of the internal risk and control system, avoiding overlaps and wastes of resources, and gaps in the activities conducted by the different actors. Therefore, there is the need to ensure that the roles and responsibilities of each participant are well defined and that these subjects cooperate and communicate enabling information flows. In the specific, this research investigated the role of the internal audit in risk management to discover whether the IA function is playing roles in its field of activity or is overlapping with the activities performed by the risk management function, reducing the effectiveness of the system.

It emerged from the assessment conducted in chapter 3 that, also for this aspects, the majority of the entities is formally complying with what required by the Codice di Autodisciplina. As already stated, this formal compliance let arise doubts on the entities' declarations. Moreover, looking at the formal compliance, it has been discovered that those companies that have been more able to provide additional information to what explicitly required by the regulator, are also part of the group of companies that scored better in the first analysis made. Therefore, the size of the organization and the sector in which the entity operates seem to have influenced the truth disclosure of a wide set of information.

When assessing the role of IA in risk management, it has been identified that entities in the sample almost never (Parmalat is the only exception) declare that their IA function executes activities that are in the scope of the risk management function. This finding is a positive sign when trying to assess if the different actors involved are cooperating in managing risks. Indeed, this result shows that the internal audit is not duplicating the job already performed (in theory) by the risk management function.

The general conclusion of the second research is that the roles assumed by the IA function seem not to overlap with those assumed by the risk management function. Indeed, while only 1 company in the sample declares that its IA performs activities normally performed by the risk management function, all entities declare that their internal auditors provide assurance on the risk and control system, and the 50% of them declares that they also provide consulting services (always maintaining the function independent).

In this thesis has not only been assessed the relationship between these two function. The further step has been to identify and assess the coordination methods implemented between the different actors, as asked from this year by the Codice di Autodisciplina.

Entities have positively responded to the new requirements of the Code to disclose information about the coordination mechanisms. However, even if the 70% of the entities in the example did it, it appears that, even in this case, companies have mainly formally complied with what required. It emerges then that, even if organizations are trying to implement the new requirement, they still have to make many efforts to actually do it.
However, even in this case, there are some exceptions and those entities that better disclose these coordination mechanisms are financial entities. Therefore, the sector of activity of the organization played a role in this analysis.

The general conclusion of this third research is that entities understand the importance of coordination and collaboration of the subjects involved and they reflect it in their clear definition of functions' roles and in the creation of continuous information flows. However, even in this study, it emerged that organizations are slowly moving to fully satisfy these needs and that the efforts to be made are still many.

General conclusion

From the CGR, ERM appears to be a best practice in risk management and, even if entities understand the relevance of having a well implemented risk management system, they still need to make a lot of work to ensure this implementation. By the way, some organizations, more than others, present a proper risk management system that seems tailored on their specific needs. Indeed, entities having a great market capitalization or operating in some specific sectors (as the financial) or having a large geographic scope resulted to have implemented better than the others a proper risk management system.

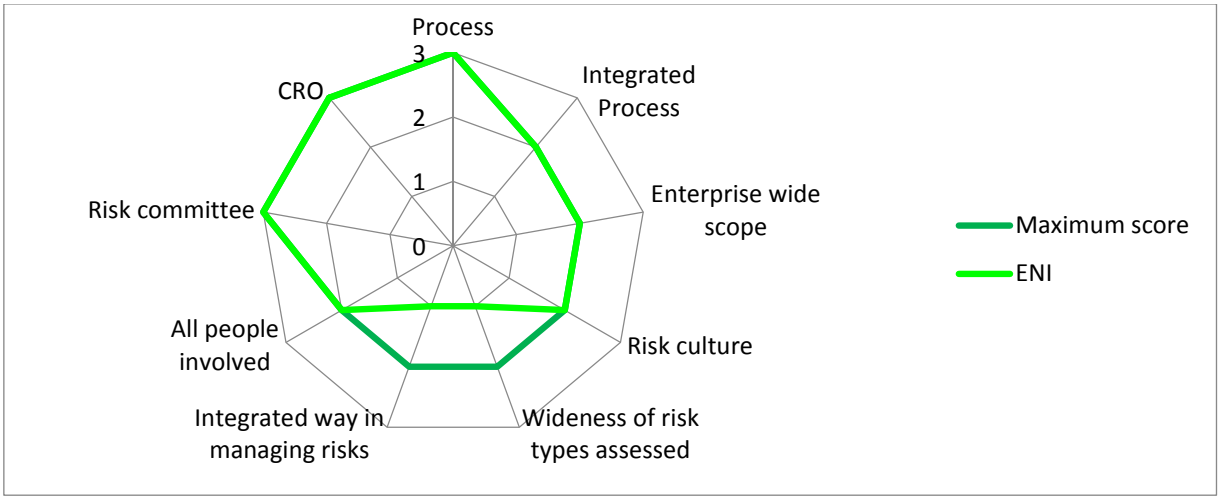
Furthermore, being the participation of many actors to risk management and their coordination two of the main aspects of ERM, it has been discovered when assessing these aspects that entities still have to make many steps to ensure a proper coordination and collaboration of the subjects

involved. Indeed, even if organizations declare to have clearly defined the role of every actor, trying to avoid overlaps in roles (as resulted by the conclusions of the second study), they appear to be deficient in declaring how these actors actually coordinate.

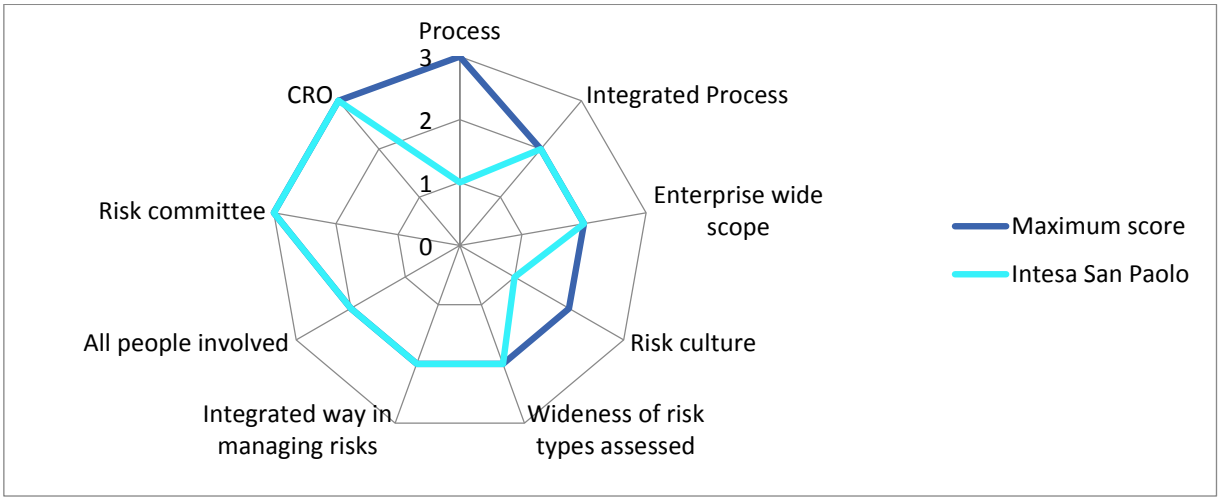
This finding is completely in line with the previous conclusion. Indeed, having already affirmed that organizations still have to work to implement a risk management system aligned to the best practices of the moment and having identified the need for coordination and collaboration between the actors involved as one of the elements of ERM, it is not a surprise then that to improve their risk management system they would have to improve also how subjects coordinate.

Appendix

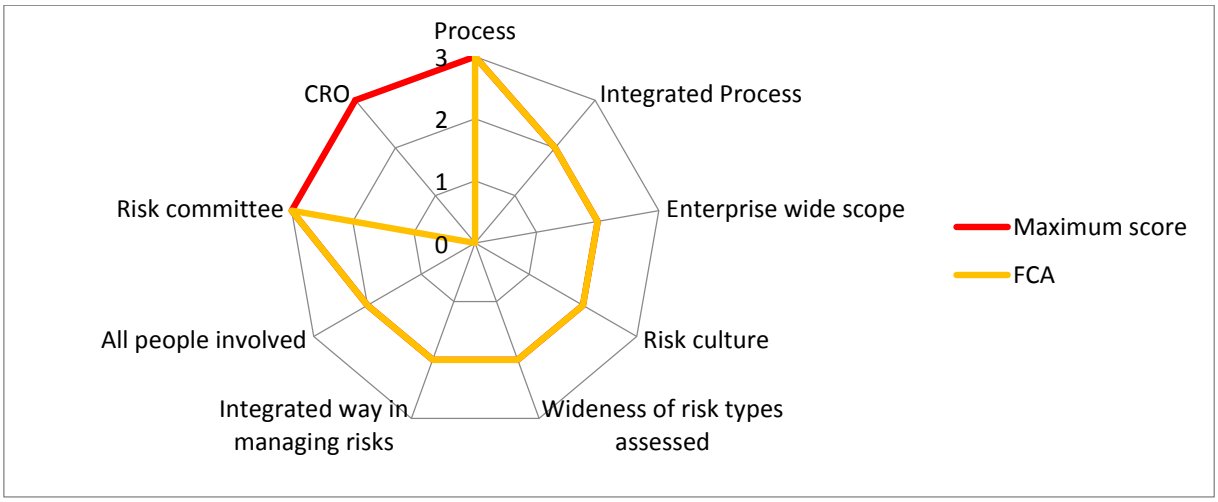
Graph A1.1: *Eni's data on ERM key elements*



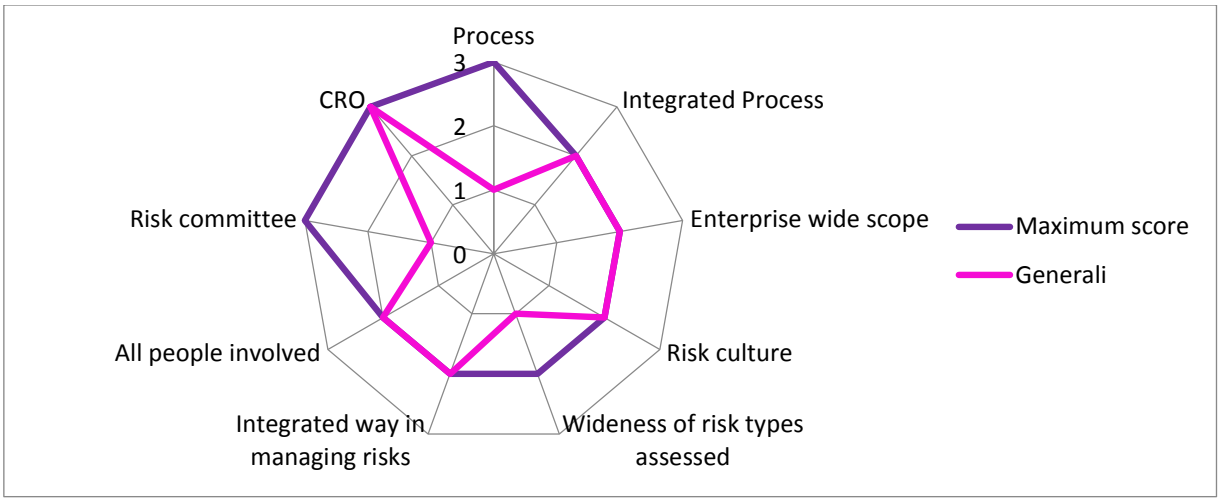
Graph A1.2: *Intesa San Paolo's data on ERM key elements*



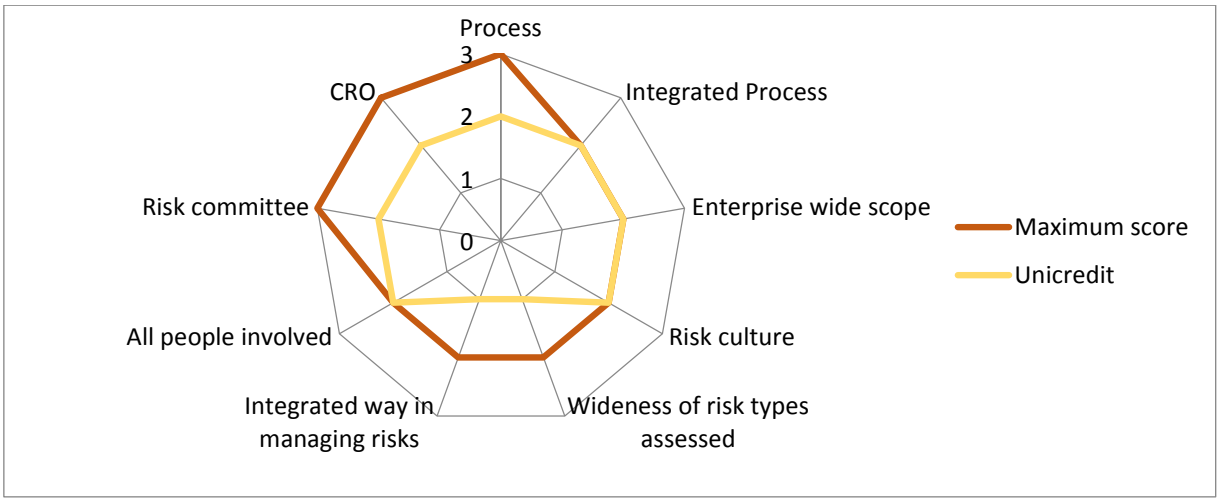
Graph A1.3: *FCA's data on ERM key elements*



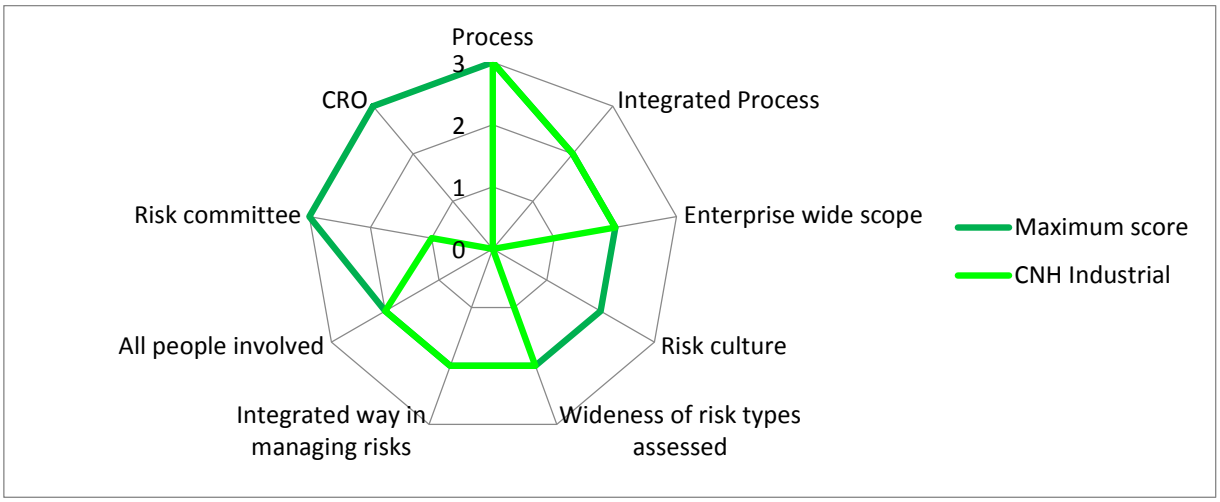
Graph A1.4: *Generali's data on ERM key elements*



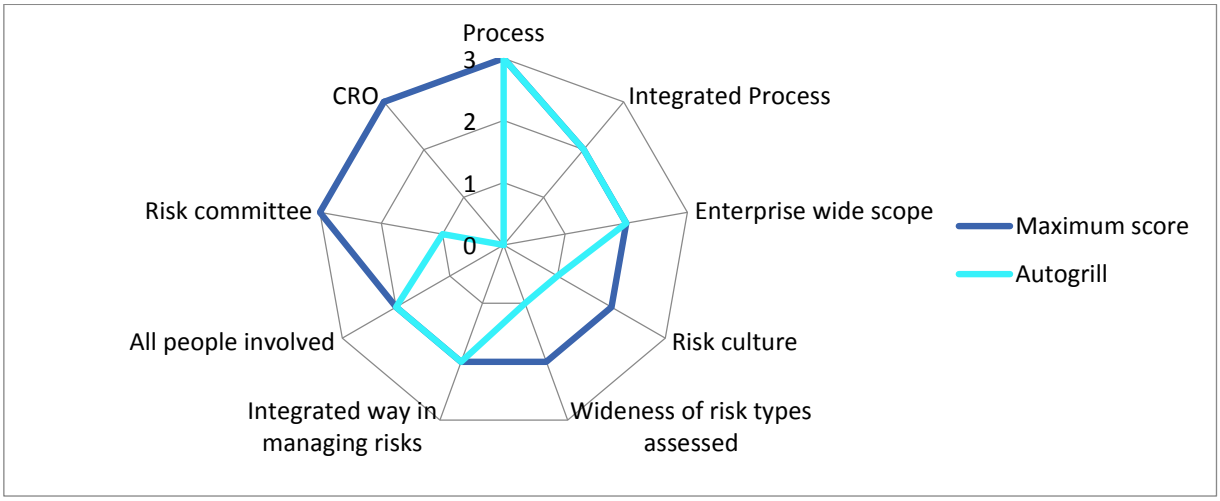
Graph A1.5: *Unicredit's data on ERM key elements*



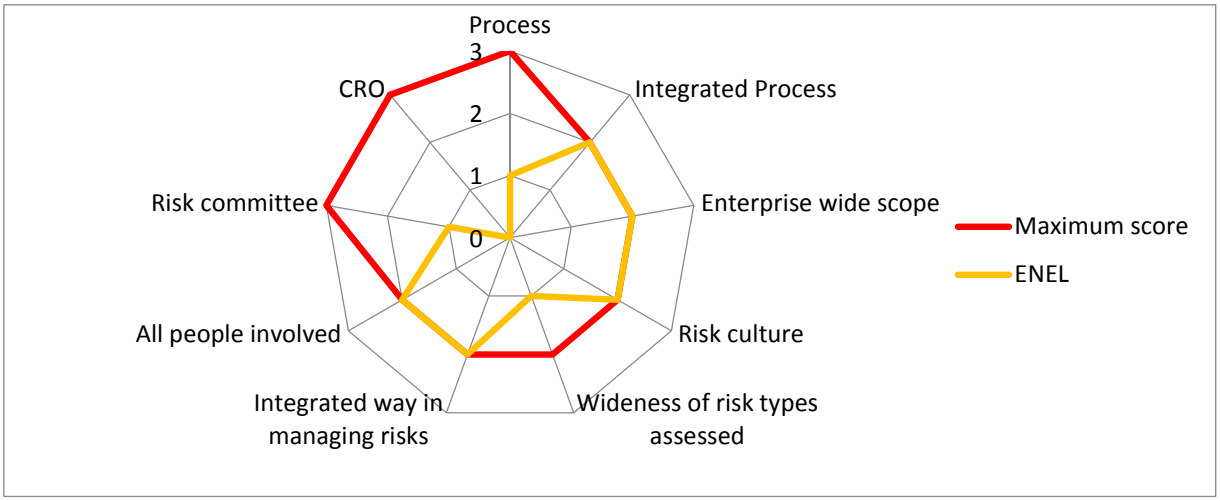
Graph A1.6: *CNH Industrial's data on ERM key elements*



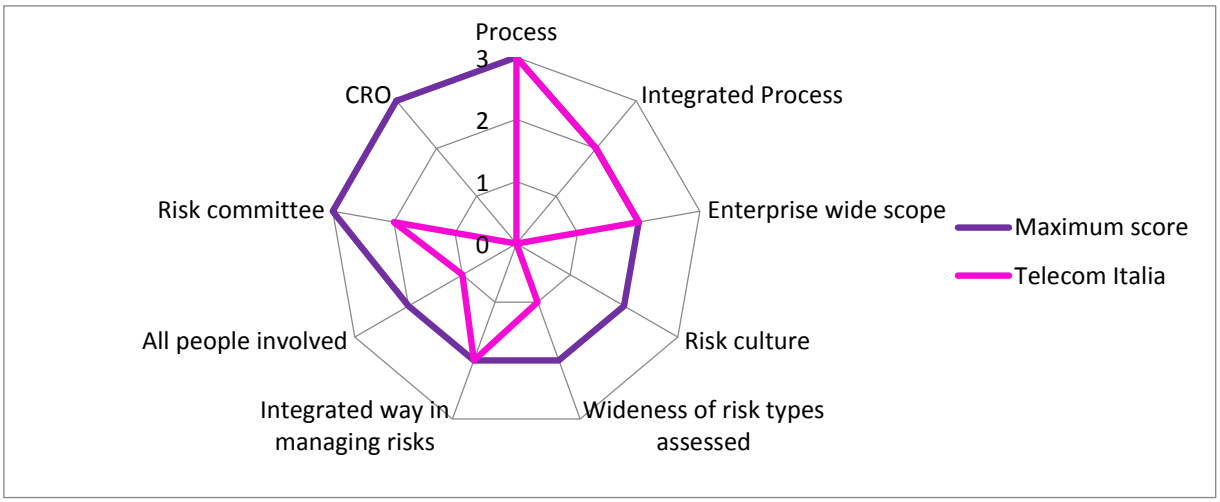
Graph A1.7: *Autogrill's data on ERM key elements*



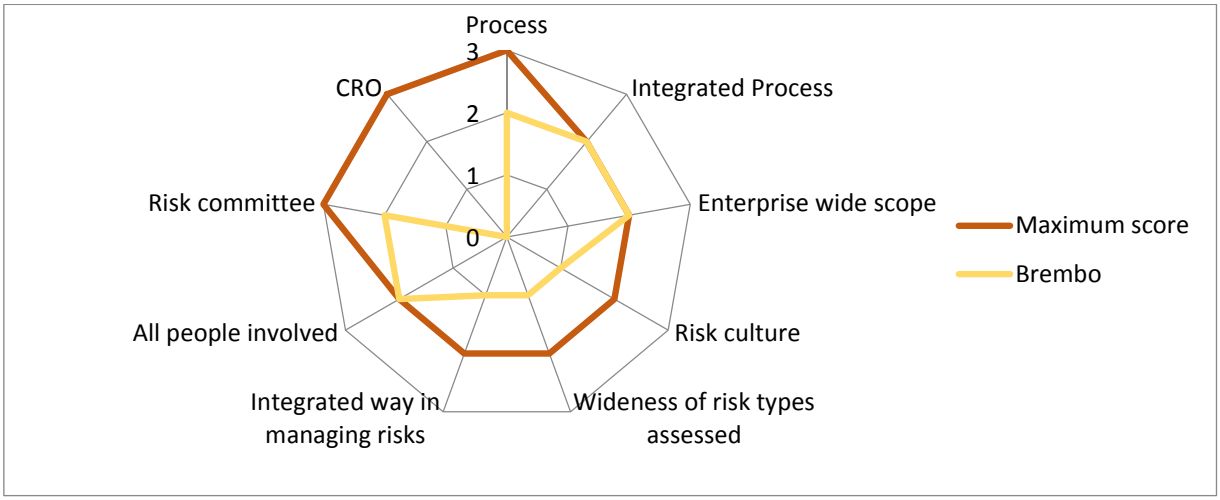
Graph A1.8: *ENEL's data on ERM key elements*



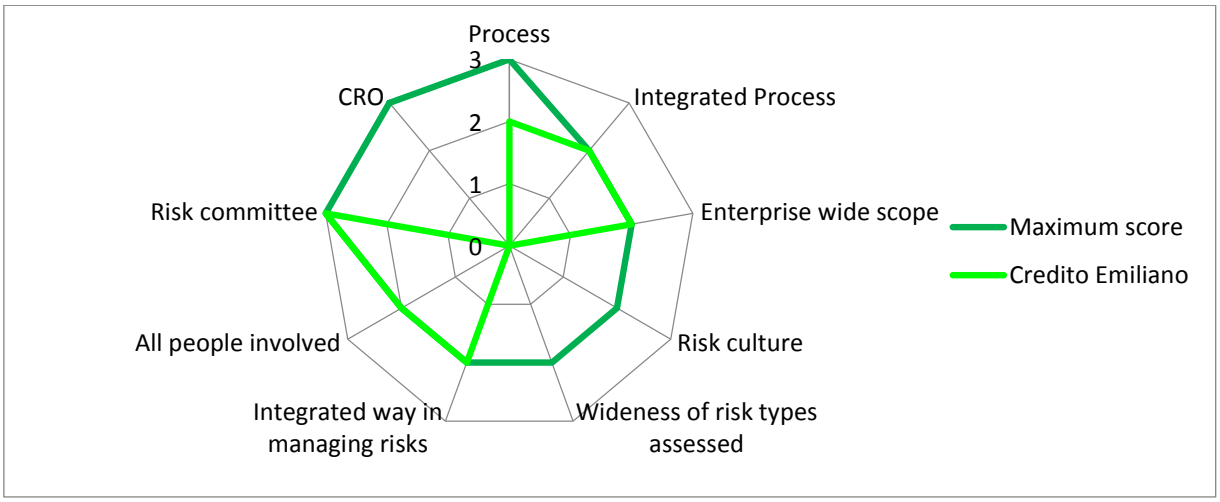
Graph A1.9: *Telecom Italia's data on ERM key elements*



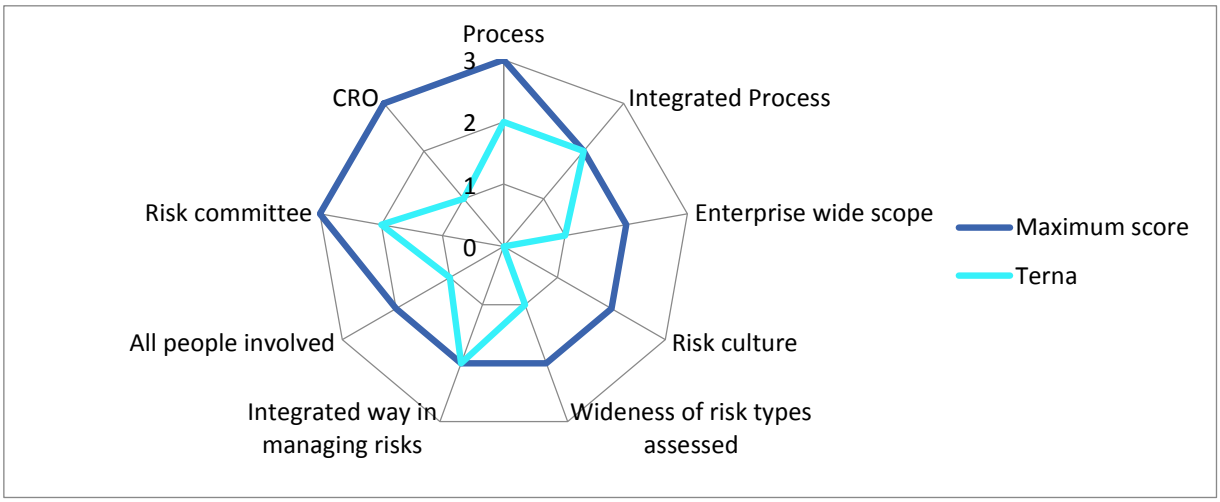
Graph A1.10: *Brembo's data on ERM key elements*



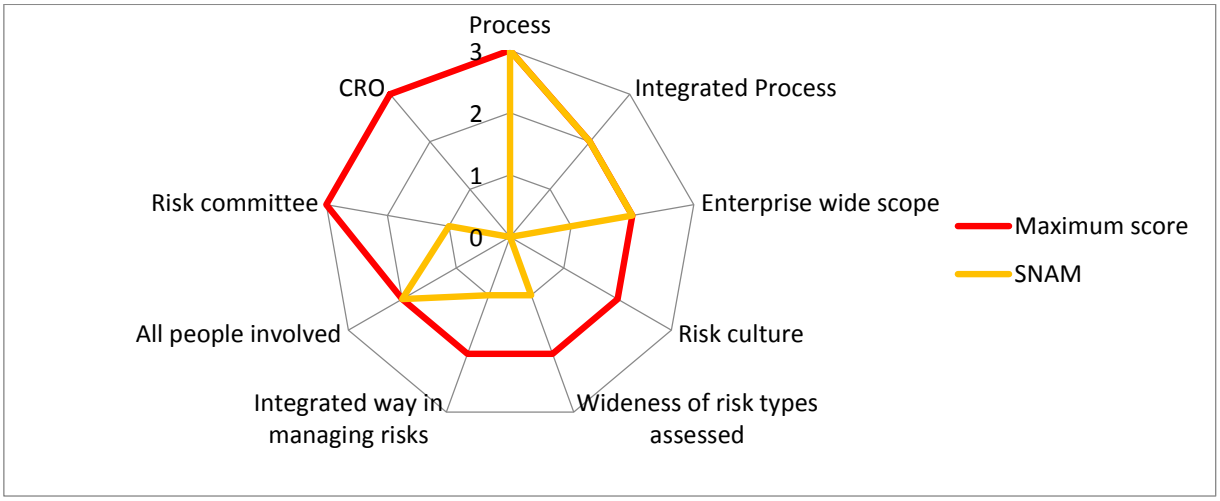
Graph A1.11: *Credito Emiliano's data on ERM key elements*



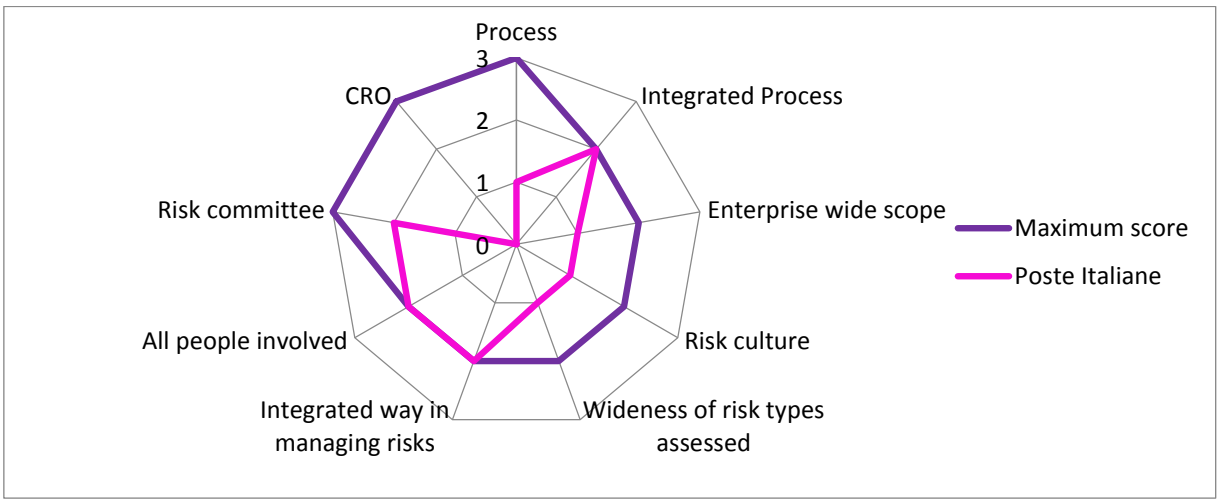
Graph A1.12: *Terna's data on ERM key elements*



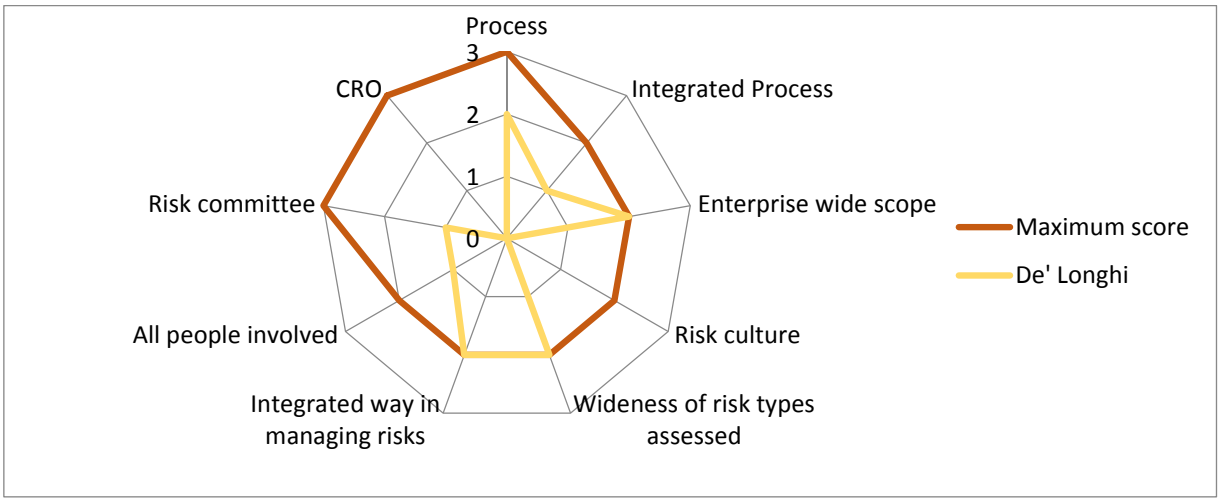
Graph A1.13: *SNAM's data on ERM key elements*



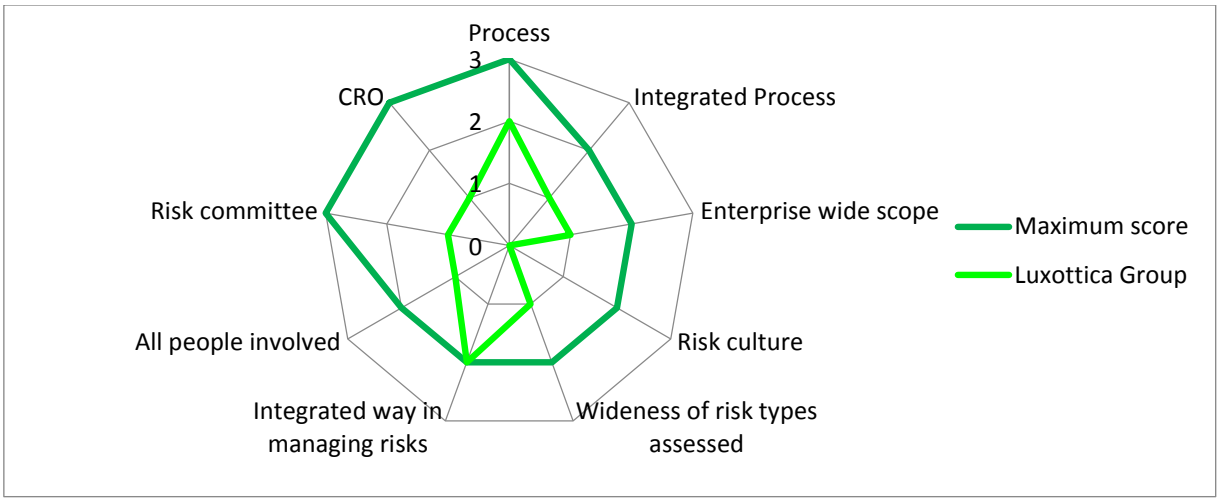
Graph A1.14: *Poste Italiane's data on ERM key elements*



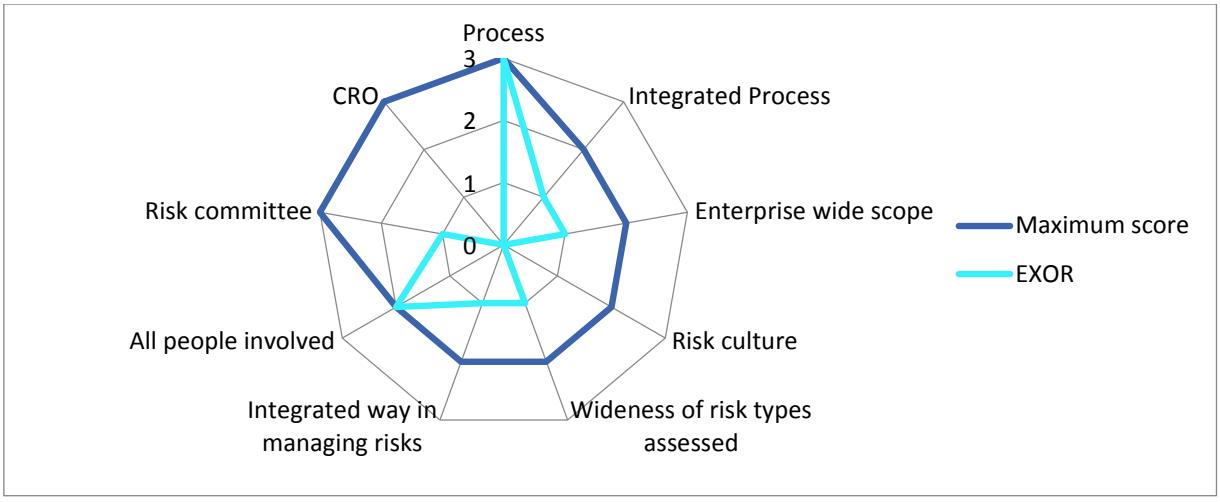
Graph A1.15: *De' Longhi's data on ERM key elements*



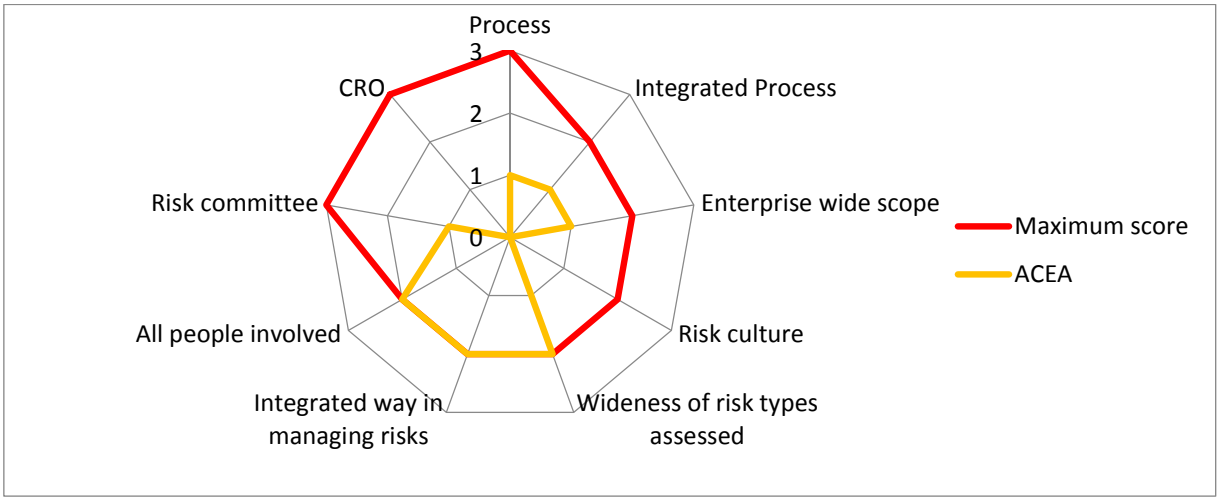
Graph A1.16: *Luxottica Group's data on ERM key elements*



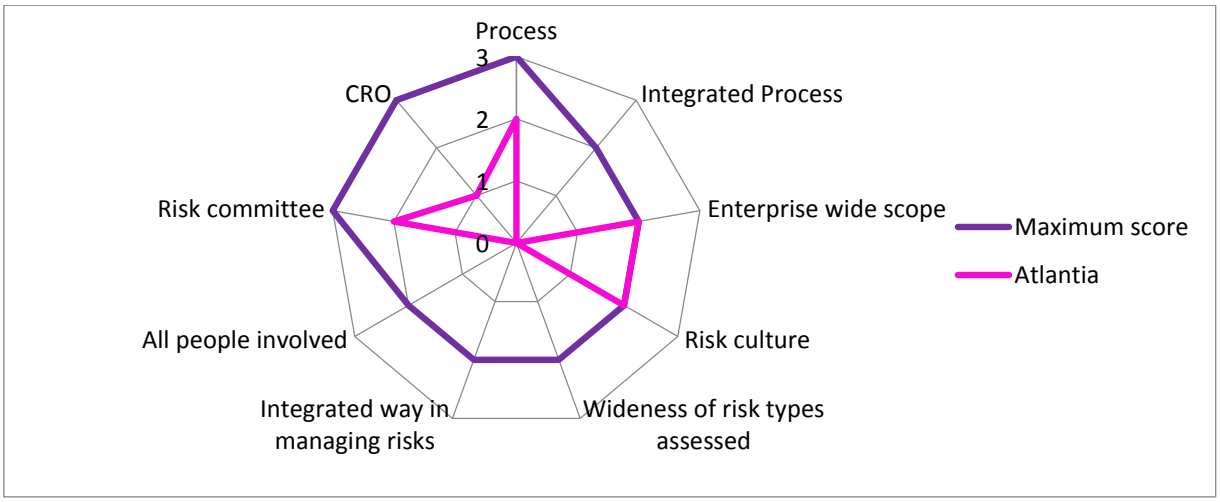
Graph A1.17: *EXOR's data on ERM key elements*



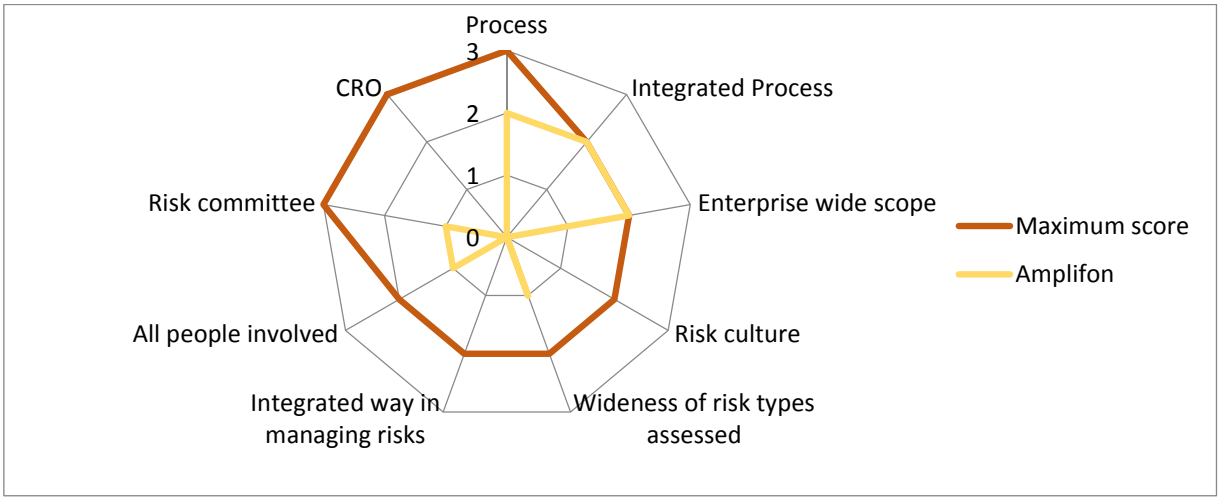
Graph A1.18: *ACEA's data on ERM key elements*



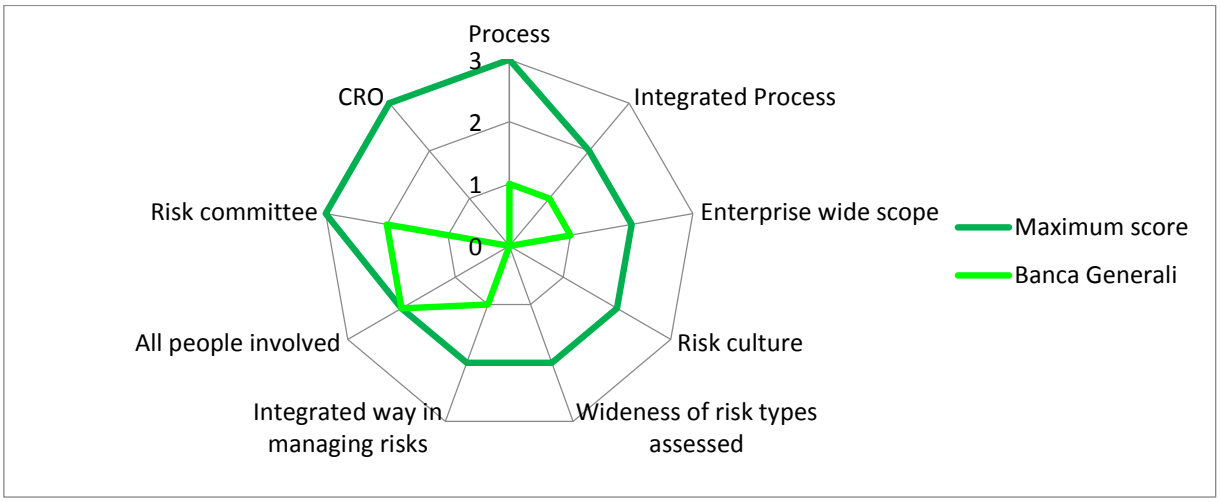
Graph A1.19: *Atlantia's data on ERM key elements*



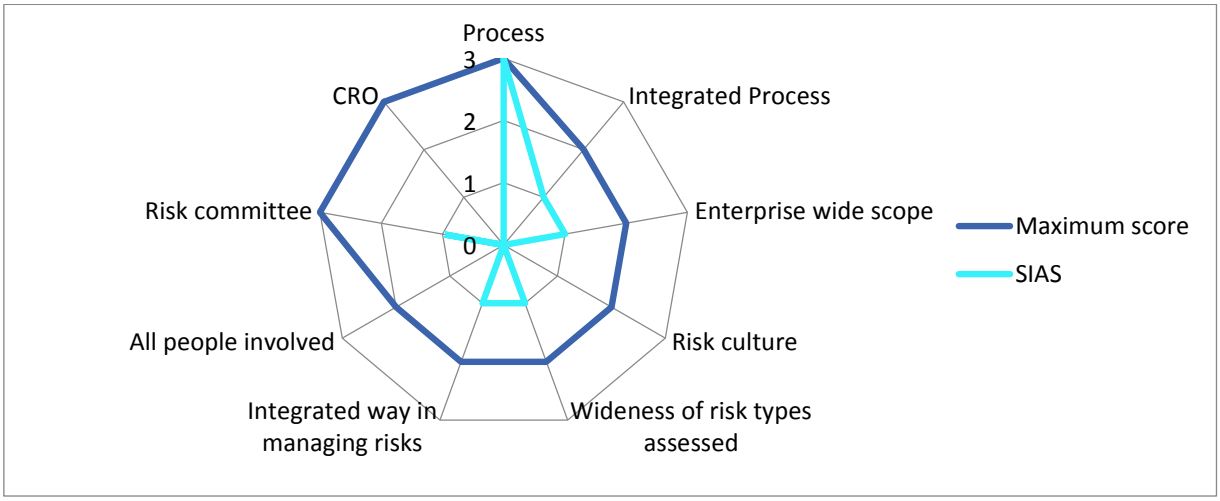
Graph A1.20: *Amplifon's data on ERM key elements*



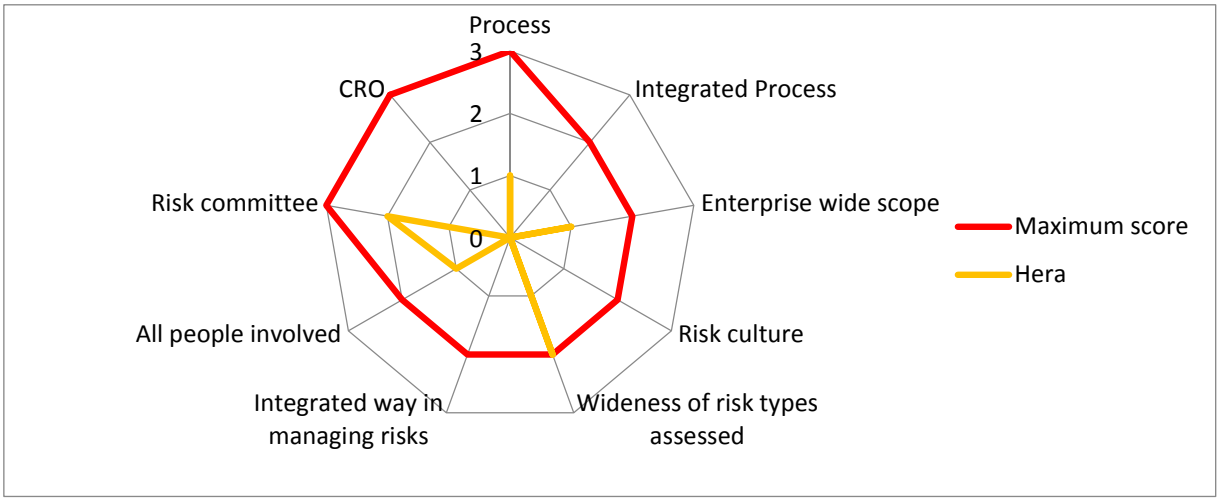
Graph A1.21: *Banca Generali's data on ERM key elements*



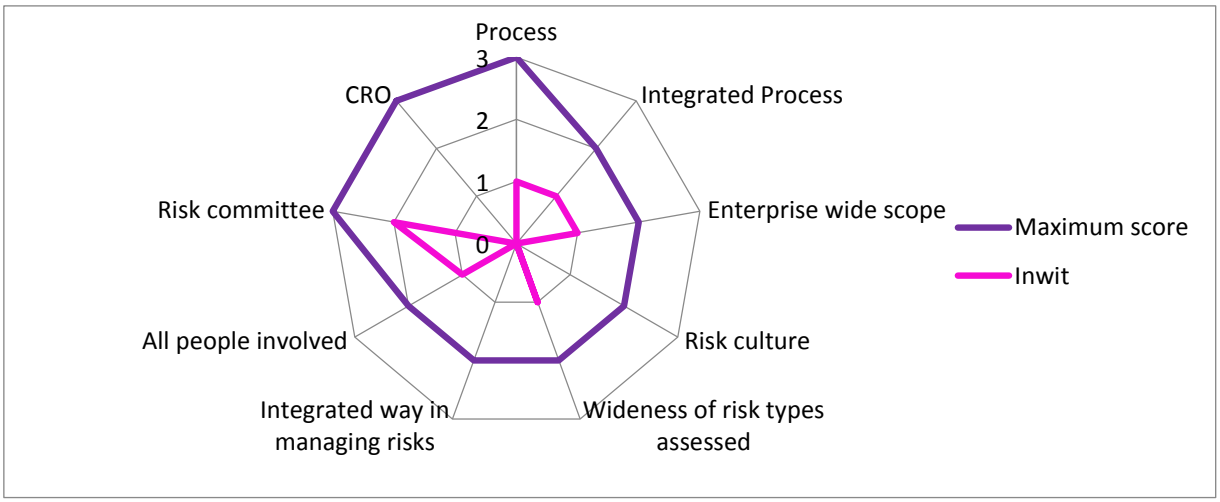
Graph A1.22: *SIAS' data on ERM key elements*



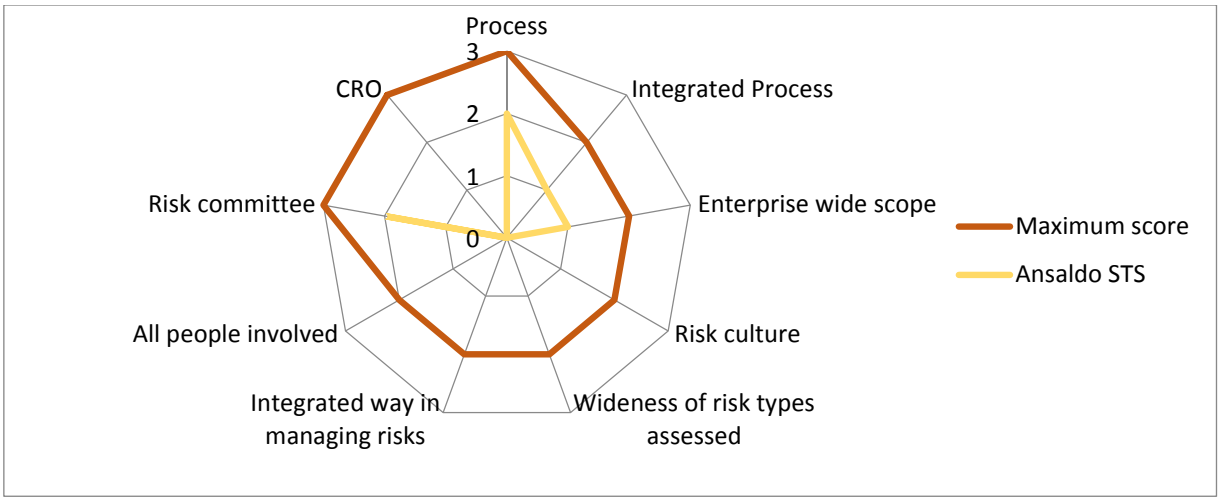
Graph A1.23: *Hera's data on ERM key elements*



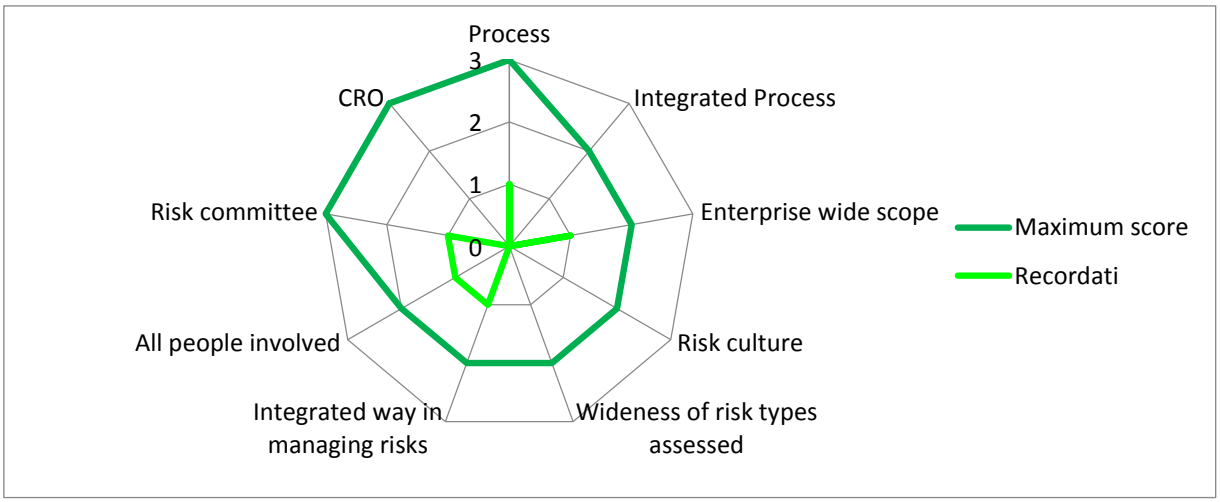
Graph A1.24: *Inwit's data on ERM key elements*



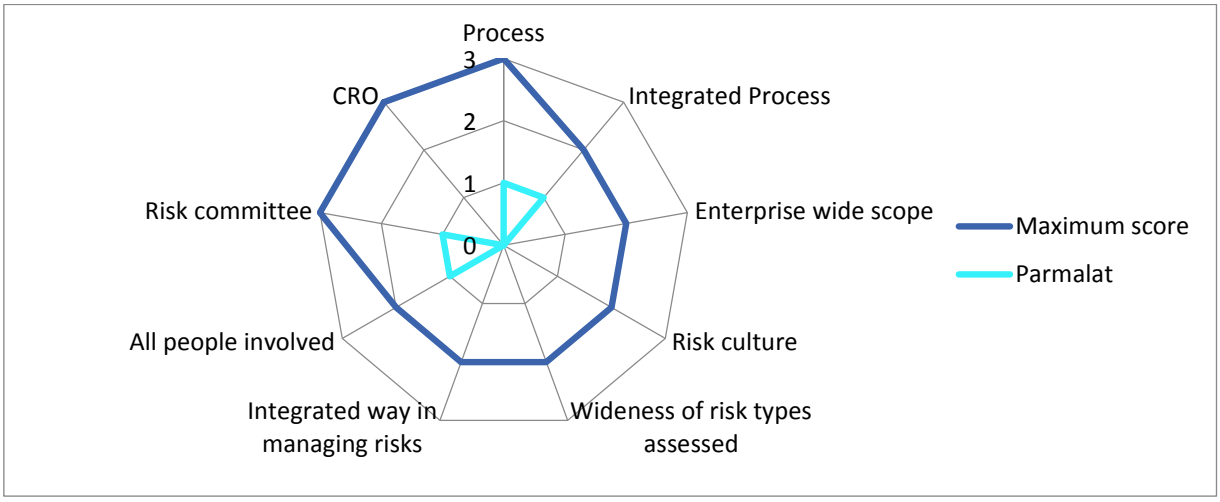
Graph A1.25: *Ansaldo STS's data on ERM key elements*



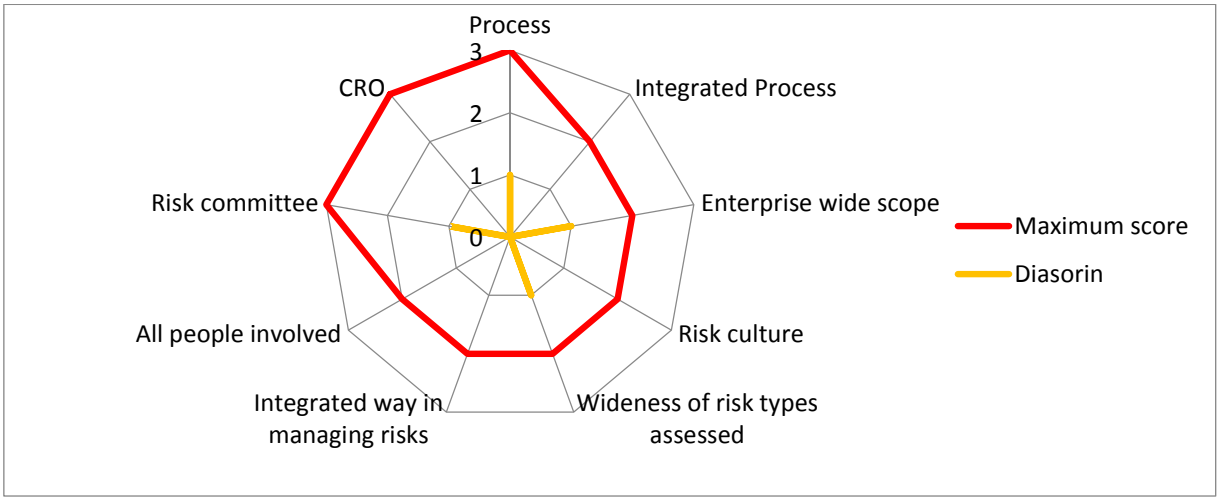
Graph A1.26: *Recordati's data on ERM key elements*



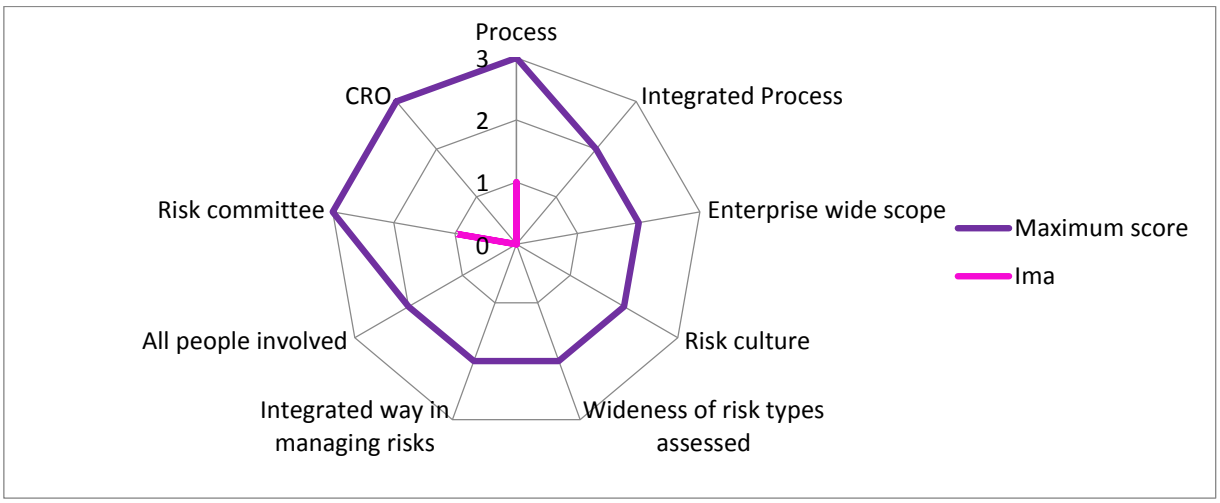
Graph A1.27: *Parmalat's data on ERM key elements*



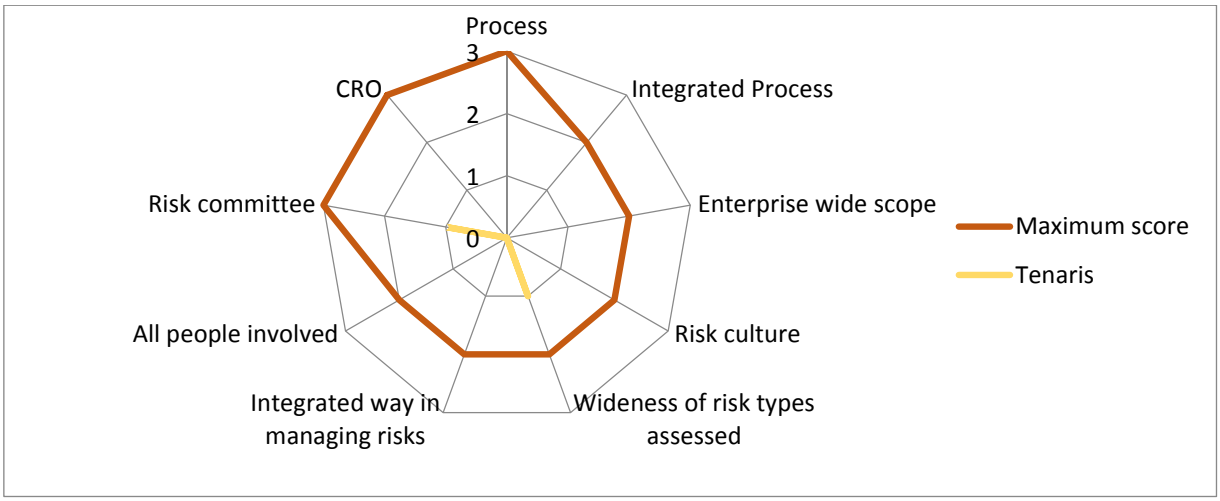
Graph A1.28: *Diasorin's data on ERM key elements*



Graph A1.29: *IMA's data on ERM key elements*



Graph A1.30: *Tenaris's data on ERM key elements*



References

Acea, (2016). "*Relazione sul Governo Societario e gli Assetti Proprietari".*

AIRMIC, Alarm, IRM, (2010). "*A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000".*

Amplifon, (2016). "*Relazione sul Governo Societario e gli Assetti Proprietari".*

ANDAF. *"Linee Guida Sistema di Controllo Interno per il Governo dei Rischi nelle PMI".*

ANRA, (2011). *"Risk Management Standards and ISO 31000".*

Ansaldo, (2016). "*Relazione del Consiglio di Amministrazione sul sistema di Corporate Governance e sull'adesione al Codice di Autodisciplina delle Società Quotate relativa all'esercizio 2015".*

Assirevi, (2016). *"L'Esercizio del Risk Oversight da parte del Consiglio di Amministrazione".*

Atlantia, (2016). *"Relazione Annuale sul Governo Societario e gli Assetti Proprietari".*

Autogrill, (2016). "*Relazione sul Governo Societario e gli Assetti Proprietari".*

Banca D'Italia, (2013). *"Disposizioni di vigilanza per le banche Circolare n. 285 del 17 dicembre 2013".*

Banca Generali, (2016). "*Relazione annuale sul Governo societario e gli Assetti Proprietari".*

Bedard, J. (2016). "Enterprise Risk Management Program Quality: Determinants, Value Relevance and the Financial Crises".

Borsa Italiana, (2015). "Format per la relazione sul Governo Societario e gli Assetti Proprietari".

Brembo, (2016). "*Relazione annuale sul Governo societario e gli Assetti Proprietari".*

Bugalla, J. & Narvaez, K. (2014). *"The Perils of Silos in Risk Management".*

Chartered Institute of Internal Auditors, (2014). *"Risk Based Internal Auditing".*

Chartered Institute of Internal Auditors, (2014). *"Risk Maturity Assessment".*

Chartered Institute of Internal Auditors, (2014). *"Production of the Audit Plan".*

Chartered Institute of Internal Auditors, (2014). *"Doing the Audit".*

CNH Industrial, (2016). "*Annual Report".*

Comitato per la Corporate Governance, (2015). *"Codice di Autodisciplina".*

CONSOB, (2013). *"I Controlli Interni nelle Società Quotate".*

COSO, (2014). *"Enterprise Risk Management – Integrated Framework"*

Corporate Governance Council, (2012). *"Risk Governance Guidance for Listed Boards".*

Credito Emiliano S.p.A., (2016). "*Relazione annuale sul Governo societario e gli Assetti Proprietari".*

Crouhy M., Dalai G., Mark R., (2014). *"The Essentials of Risk Management".*

De' Longhi S.p.A., (2016). "*Report on Corporate Governance and the Ownership Structure pursuant art. 123-bis of the TUF".*

Diasorin, (2016). *"Relazione annuale sul Governo societario e gli Assetti Proprietari ai sensi dell'art. 123-bis del TUF".*

Enel, (2016). "*Relazione annuale sul Governo societario e gli Assetti Proprietari".*

Enel, (2016). "*Linee di indirizzo del Sistema di Controllo Interno e Gestione dei Rischi".*

ENI, (2016). "*Relazione annuale sul Governo societario e gli Assetti Proprietari".*

EXOR, (2016). "*Relazione sulla Corporate Governance".*

FCA, (2016). "*Annual Report".*

Generali, (2016). "*Relazione annuale sul Governo societario e gli Assetti Proprietari".*

Gruppo Hera, (2016). "*Bilancio consolidato e separato al 31 dicembre 2015".*

IIA, (2004). *"The Role of Internal Auditing in Enterprise Wide Risk Management".*

IIA, (2012). *"Coordinating Risk Management and Assurance".*

IIA, (2013). "*The Three Lines of Defense in Effective Risk Management and Control".*

IIA, (2015). *"Leveraging COSO across the Three Lines of Defense".*

IIA, (2016). *"Internal Audit and the Second Line of Defense".*

IIA, (2016). *"White Paper – Integrated Risk-Based Internal Audit".*

IMA S.p.A., (2016). "*Relazione annuale sul Governo societario e gli Assetti Proprietari ai sensi dell'art. 123-bis del TUF".*

Intesa SanPaolo, (2016). "*Relazione annuale sul Governo societario e gli Assetti Proprietari".*

Inwit, (2016). "*Relazione annuale sul Governo societario e gli Assetti Proprietari dell'esercizio 2015 di Infrastrutture Wireless Italiane S.p.A.".*

Luxottica Group S.p.A., (2016). "*Relazione annuale sul Governo societario e gli Assetti Proprietari ai sensi dell'art. 123-bis del TUF".*

Parmalat S.p.A., (2016). "*Relazione annuale sul Governo societario e gli Assetti Proprietari".*

Poste Italiane S.p.A., (2016). "*Relazione sul Governo Societario e gli Assetti Proprietari".*

Poste Italiane S.p.A.. "Linee Guida sul *Sistema di Controllo Interno e Gestione dei Rischi".*

Recordati, (2016). "*Relazione sul Governo Societario e gli Assetti Proprietari".*

Segal, S. (2011). *"Corporate Value of Enterprise Risk Management".*

Sekerci, N. (2011). *"Does Enterprise Risk Management Create Value for Firms?: Evidence from Nordic Countries".*

Sias, (2016). "*Relazione annuale sul Governo societario e gli Assetti Proprietari ai sensi dell'art. 123-bis del TUF".*

SNAM, (2016). "*Relazione sul Governo Societario e gli Assetti Proprietari 2015".*

Telecom Italia S.p.A., (2016). "*Relazione sul Governo Societario e gli Assetti Proprietari dell'esercizio 2015 di Telecom Italia S.p.A.".*

Tenaris, (2016). "*Annual Report".*

Terna Group, (2016). "*Relazione sul Governo Societario e gli Assetti Proprietari".*

Unicredit S.p.A., (2016). "*Relazione sul Governo Societario e gli Assetti Proprietari".*

Summary

During the last decades, the attention that regulators, entities and stakeholders addressed to risk management changed drastically because of the occurrence of specific events, as financial crises and natural catastrophic events, and because of a new diffuse perception about risk. Indeed, while risk was considered before only as a negative element and the potential positive effects of the upside volatility were not accounted, nowadays entities understand that a risk might represent a resource and an opportunity if well managed. Therefore, even the way in which risks are managed had to change to reflect this different risk perception.

Traditional risk management systems were mainly dependent on a historical-data treatment of risk and mainly focused on financial risks (failing to consider the wide range of risk types). Moreover, they were mainly based on a silos-approach in managing risks, and they were not conducting a risk-return analysis able to support decision-making and to ensure the maximization of shareholders' value. Nowadays, the best practice in risk management is Enterprise Risk Management (ERM). This practice is defined by COSO (2004) as "a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives". Therefore, as emerge by the definition above, this best practice seems to overcome the typical issues of the traditional systems.

There is a wide set of guidelines, principles and standards about ERM, and, because of it, it might be believed that this practice is widely implemented by entities.

The first chapter of this thesis presents a study on ERM conducted to assess, over a sample of 30 Italian listed companies, if this best practice is actually diffuse or if it remains only a theoretical suggestion.

After presenting all the possible methodologies to conduct the analysis, it is described the one chosen. Gathering information directly from the entity through a careful analysis of the Corporate Governance Reports (CGR) has been considered as the best way to obtain trustful information and to reduce the subjectivity that could otherwise be faced when letting employees discuss and score their risk management system. However, because of this methodology, it has to be kept in mind

while reading this thesis that any evaluation has been made on the base of what entities declared in their official documents.

Each of the three studies conducted in this thesis has used as sample of companies a heterogeneous group of 30 Italian listed companies having different sizes (in terms of market capitalization) and exercising their activities in different sectors. Indeed, looking at the market capitalization, the sample is composed by the first fifteen entities of the FTSE MIB basket and by the first fifteen entities of the ITALIAN MID CAP basket. Looking at the macro sector in which they operate, it is possible to count 7 entities operating in Financial, 5 in Utilities, 1 in Oil & Gas, 5 in Industrials, 5 in Consumer Goods, 1 in Consumer Services, 3 in Health Care, 2 in Telecommunication and 1 in Basic Materials.

To assess the level of implementation of ERM, a group of key elements of enterprise risk management has been identified in line with COSO's definition, and a set of scores has been assigned to each of these elements. Whereupon, it has been assessed if and in which measure these elements were declared by entities in their CGRs.

Therefore, with the information obtained from the analysis conducted, it has been built a table (shown below) containing the partial scores and the sum of the partial scores gathered by each company. On the base of the sum of the partial scores, entities have been ranked from the one that totalized the biggest score, meaning that it has "expressed" the most mature risk management system, until the one with the lowest score, meaning that the "declared" level of implementation of the system is lower.

Furthermore, in the last row of the table are shown the average score totalized for each key element. This additional row has been added in order to check which are the factors that most easily have been implemented and which are those still requiring many efforts by entities.

Red cells identify elements whose average is lower than the mean of the possible scores attributed to them, orange cells identify elements whose average is a bit higher than the mean of the possible scores attributed, and green cells identify elements whose average is greater than the mean of the possible scores attributed.

Entity	Process	Integrated process	Enterprise wide scope	Risk culture	Wideness of risk types assessed	Integrated way in managing risks	All people involved	Risk Committee	CRO	Tot
ENI	3	2	2	2	1	1	2	3	2	**18**
Intesa San Paolo	1	2	2	1	2	2	2	3	3	**18**
FCA*	3	2	2	2	2	2	2	3	0	**18**
Generali	1	2	2	2	1	2	2	1	3	**16**
Unicredit	2	2	2	2	1	1	2	2	2	**16**
CNH Industrial	3	2	2	0	2	2	2	1	0	**14**
Autogrill	3	2	2	1	1	2	2	1	0	**14**
ENEL	1	2	2	2	1	2	2	1	0	**13**
Telecom Italia	3	2	2	0	1	2	1	2	0	**13**
Brembo	2	2	2	1	1	1	2	2	0	**13**
Credito Emiliano	2	2	2	0	0	2	2	3	0	**13**
Terna	2	2	1	0	1	2	1	2	1	**12**
Snam	3	2	2	0	1	1	2	1	0	**12**
Poste Italiane	1	2	1	1	1	2	2	2	0	**12**
De' Longhi	2	1	2	0	2	2	1	1	0	**11**
Luxottica Group	2	1	1	0	1	2	1	1	1	**10**
Exor	3	1	1	0	1	1	2	1	0	**10**
Acea	1	1	1	0	2	2	2	1	0	**10**
Atlantia	2	0	2	2	0	0	0	2	1	**9**
Amplifon	2	2	2	0	1	0	1	1	0	**9**
Banca Generali	1	1	1	0	0	1	2	2	0	**8**
SIAS	3	1	1	0	1	1	0	1	0	**8**
Hera	1	0	1	0	2	0	1	2	0	**7**
Inwit	1	1	1	0	1	0	1	2	0	**7**
Ansaldo STS	2	1	1	0	0	0	0	2	0	**6**
Recordati	1	0	1	0	0	1	1	1	0	**5**
Parmalat	1	1	0	0	0	0	1	1	0	**4**
Diasorin	1	0	1	0	1	0	0	1	0	**4**
Ima	1	0	0	0	0	0	0	1	0	**2**
Tenaris**	0	0	0	0	1	0	0	1	0	**2**
Average	1.86	1.34	1.45	0.55	0.97	1.17	1.34	1.60	0.43	
Mean	1.5	1	1	1	1	1	1	1.5	1.5	

The main conclusions obtained by the first study of this thesis are:

- Entities seem to understand the relevance of a well implemented ERM, but the majority of them appear more focused on formally comply with the directives rather than on making efforts to actually implement a good risk management system. A formal compliance let arise doubts on the goodness for the entities' statements implementation. It appears

indeed dubious that these organizations, even being different and having different governance structures, report exactly the same aspects when describing the SCIGR.

- Evidence of the formal compliance is provided when observing that the key elements that recorded an average higher than the mean were exactly those more regulated and for which entities were obliged to disclose information in order to comply with the Code.
- Some specific aspects of the entities influenced their ranking. Indeed, it resulted that bigger companies, because of their greater complexity and need to ensure protection against risk and because of their biggest amount of resources available, implement more mature risk management systems. Other aspects that emerged to influence the result of the research have been the sector in which the entity operates and the geographic scope that the entity has.

After that the ERM has been described and that its implementation within the sample of Italian listed entities has been assessed, it is introduced in chapter 2 the theme of risk governance. This latter represents the architecture within which risk management operates" (Corporate Governance Council, 2012). Identifying how roles and responsibilities within ERM are settled, divided and assigned to people part of the organization, risk governance ensures a suitable level of control on the implementation and execution of the activities needed to manage risk.

Even if it is not possible to generalize because every entity might adopt a different risk governance, there are some roles and responsibilities that every entity should have. Chapter 2 shows some of the main actors involved in risk governance (BoD, "Comitato Controllo e Rischi", Director of the SCIGR, CRO) and their responsibilities. In describing the roles assumed by these actors and their relative duties, great reference is made to the Codice di Autodisciplina for Italian Listed Companies.

Moreover, when presenting the internal audit function and the risk management function, it goes more in detail describing the Three Lines of Defense Model. This latter involves the participation of three groups of actors, each one of them resulting fundamental for the good output of the risk management system. Risk owners (1st line) are the ones better knowing the business and the issues arising from it. They are the most appropriate to identify risks, assess them, mitigate them and then monitor them. Risk managers (2nd line) are needed to ensure coordination among the actions undertaken by the different risk owners. Their intervention is fundamental to train and

guide risk owners in the execution of their duties, and to let them contribute to the respect of the risk limits attributed to their function and of the general risk appetite set for the organization. Finally, internal auditors (3rd line) are fundamental to ensure that the system receives independent and objective assessments to guarantee that the control and risk management system is implemented properly and that the strategic objectives are met.

The Model gives an easy and effective method to increase communication on risk management and control through the definition of specific roles and responsibilities. When the lines of defense are properly implemented, it should be reduced the possibility of gaps in control and of duplication actions, and there should be a greater probability to proper address and manage risk and control.

The role that internal audit has in risk management is further analyzed in the 3rd chapter. Indeed, after an initial explanation of the necessity to ensure independence and objectivity to the internal audit function, it is presented the "fan of roles" that IA should undertake/undertake with safeguards/or not undertake. This fan, contained in a Position Paper of the IIA (2004), shows in the left side the assurance roles (core roles of the IA), in the center the consulting services roles (to be undertaken only with safeguards to the independence and objectivity of this function) and in the right side those roles that are normally played by the risk management function. Internal audit might manly provide assurance on three important aspects: on the effectiveness of the risk management and internal control system, on the proper management of key risks faced by the entity, and on the appropriateness of the assessment conducted to identify and manage all risks faced. Instead, the consulting services provided by this function can be classified in two main groups. The first one contains advices directed to the enhancement of the control and risk management system (overall advise on the process), while instead the second one contains those advices directed to the enhancement of the risk identification, measuring, mitigation and monitoring through a direct help provided to management and top management.

From the fan of roles and from the Three Lines of Defense Model, it is clear the necessity of both the risk management and the internal audit function in managing risks, as well as the necessity to clearly define roles and responsibilities to them assigned so that overlaps or gaps are avoided. Risk management and internal audit should be independent from each other, but at the same time should cooperate.

Therefore, because of the focus that internal audit has in risk management, it is possible to refer to the activity of this function as "Risk Based Internal Auditing", (Chartered Institute of Internal Auditors, 2014). RBIA is a mechanism that relates the IA activities to the risk management framework applied to the entire organization.

Once that the theoretical elements on which base the 2nd study of this thesis have been given, in this chapter are assessed the roles that the IA function of the 30 Italian listed companies actually plays in terms of risk management. This research has been based as well on the Corporate Governance Reports. For every entity it was looked in the report for the declaration produced by each organization in relation to the audit activities conducted during 2015 and in relation to responsibilities that this function generally has. Furthermore, on the base of this information, reported for each entity in table 3.1, it has been assessed which kind of roles the IA function of these organizations is actually undertaking.

The main conclusions obtained from the second study of this thesis are:

- Almost all entities appear to formally comply with what required by the Codice di Autodisciplina for the internal audit (7.C.5). This formal compliance not only let appear the entities' declarations ambiguous, but it let all roles assumed by this function result as "assurance". Indeed, the Criteria 7.C.5 identifies mainly an assurance role for this function.
- Only one company of the sample (Parmalat) has the IA function that undertakes roles that should be attributed to the risk management function. Instead, the 50% of these entities declare that their IA functions not only provide assurance, but also consulting services.
- Only the 20% of these entities resulted to enlarge the description provided appearing to not only formally comply. Furthermore, it has been assessed that elements as the size and the sector in which the entity operates have influenced this result.

As emerged in what described above, the subjects involved in risk governance are numerous and each one responds and is accountable for the responsibilities to him attributed. Their expertise and their contribution are fundamental for the good output of the system. However, what results more fundamental is to ensure that coordination and communication mechanisms are in place to

allow these subjects to share information and dispose of all the data needed to exercise their activities and facilitate the organization in exploiting the opportunities arising and reaching the objectives set in the strategic plan.

The concept of ensuring an efficient and effective risk management and control system where overlaps and gaps are avoided has assumed great relevance in the last years. Moreover, starting from this year, the Codice di Autodisciplina has requested companies to explicitly declare the coordination methods implemented.

This thesis investigated also how entities are actually coping with this new requirement and how much relevance they give to the coordination between the actors involved. As done with the other studies, before to start the research, a wide description is provided of the principles, standards and guidelines about coordination available to entities.

This 3rd and last research investigated the coordination mechanisms implemented by the sample of the 30 Italian listed companies. This study has been conducted on the base of what these organizations reported in their CGRs in the dedicated paragraph (required starting from this year by the Code).

The table below reports the results obtained when assessing which types of coordination mechanisms these entities implemented. For simplicity and space reasons, in the head row are not shown the coordination mechanisms titles. Instead, in the head row are contained some alphabetic letters that correspond to specific mechanisms according to the matches below:

A – Spread of a common language

B – Adoption of common and shared evaluation methods and instruments

C – Creation of continuous information flows

D – Creation of institutional occasions in which functions can meet to coordinate

E – Definition of the roles and responsibilities attributed to each function

F – Creation of the document required by Banca D'Italia (described in paragraph 3.4)

Entity	A	B	C	D	E	F	Notes
ENI							
ENEL			x				2nd line refers to the 3rd the issues to be assessed and the 3rd communicate results to the parts involeved.
Intesa San Paolo	x	x	x	x			
Luxottica Group							
Generali							
Atlantia			x				Coordination of the information flow is assigned to the CEO.
Unicredit		x	x	x	x	x	Creation of the "Documento degli Organi Aziendali e delle Funzioni di Controllo" required by BI. Managers can share information during the managerial committee dedicated to control topics. Very good also the coordination between 2nd and 3rd line of defense.
Snam							
Tenaris							
Telecom Italia					x		The paragraph assessed reports a clear definition of all the roles and responsibilities attributed to each function.
Terna			x	x	x		Widely described roles and responsibilities attributed to each function, and all the flows and meeting occasions that are put in place.
Poste Italiane	x	x	x	x			Impressing the attention Poste pays to report all the different information flows.
CNH Industrial							
Exor					x		It is declared that roles are analytically assigned
FCA							
Recordati				X	x		Widely described all the occasions when the subjects meet. It seems to focus more on these specific situations rather than on a continuous flow of information.
Parmalat							
Hera			x	x			Widely described all the occasions when the subjects meet. Creation of a risk committee that provides guidance on the strategy to follow in dealing with risks.
De' Longhi			x		x		Widely described all roles and responsibilities attributed to the different functions.
Brembo			x	x	x		Identified the roles and responsibilities assigned to some specific functions and is described how, in explicating these duties, the function reports to and communicate with other ones.
Diasorin			x				Coordination of the information and of the parts involved is assigned to the CEO.
Acea			x	x			
Banca Generali			x	x	x		Described the presence of specific meetings where managers coordinate and of information flows (through reporting). Roles and responsibilities are identified.

Inwit					x		
Ima				x			
Credito Emiliano	x	x	x		x	x	Creation of the "Documento degli Organi Aziendali e delle Funzioni di Controllo" required by BI.
Ansaldo STS			x		x		Described the roles involved.
SIAS				x	x		Cited the reporting activities of the subjects involved.
Amplifon							
Autogrill					x		
Total	**3**	**4**	**14**	**11**	**13**	**2**	

The main conclusions obtained by the 3rd study of this thesis are:

- 21 out of the 30 organizations (equal to a **70%**) have complied with the Code and have reported in a dedicated paragraph the coordination mechanisms implemented within the entity. Even if not the entire sample has accomplished with the new requirements, the number of organizations that positively responded to the new request (even if sometimes they appear only to do it formally) can be considered satisfactory. Indeed, being it the first year in which entities had to explicitly provide this information, to obtain a number greater than the half of the companies of the sample shows that they are positively responding to the new requirements.
- The majority of the entities have mainly formally complied with what required, providing the description of the roles involved and declaring the presence of information flows. However, the coordination methods shown appear many times general and not described in detail. It emerges then that, even if organizations are trying to implement the new requirement, they still have to make many efforts to actually do it;
- The coordination methods that mostly recurred in the CGR are "the clear definition of roles and responsibilities" (that avoids gaps and overlaps) and "information flows and institutional meetings/reporting" (that allow the coordination through sharing of results, data and information);
- Financial entities seem to better implement coordination mechanisms. Indeed, the organizations that scored the best, declaring all at least 4 out of the 6 mechanisms investigated, are those organizations operating in the financial sector. These entities comply with the regulation of their sector and for this reason they perform much better than the others. As it is well known, the financial sector is much more regulated than other ones and it is not a surprise that these entities better describe their coordination methods.

General conclusion

From the CGR, ERM appears to be a best practice in risk management and, even if entities understand the relevance of having a well implemented risk management system, they still need to make a lot of work to ensure this implementation. By the way, some organizations, more than others, present a proper risk management system that seems tailored on their specific needs. Indeed, entities having a great market capitalization or operating in some specific sectors (as the financial) or having a large geographic scope resulted to have implemented better than the others a proper risk management system.

Furthermore, being the participation of many actors to risk management and their coordination two of the main aspects of ERM, it has been discovered when assessing these aspects that entities still have to make many steps to ensure a proper coordination and collaboration of the subjects involved. Indeed, even if organizations declare to have clearly defined the role of every actor, trying to avoid overlaps in roles (as resulted by the conclusions of the second study), they appear to be deficient in declaring how these actors actually coordinate.

This finding is completely in line with the previous conclusion. Indeed, having already affirmed that organizations still have to work to implement a risk management system aligned to the best practices of the moment and having identified the need for coordination and collaboration between the actors involved as one of the elements of ERM, it is not a surprise then that to improve their risk management system they would have to improve also how subjects coordinate.