



UNIVERSITA' DEGLI STUDI DI PADOVA

**DIPARTIMENTO DI SCIENZE ECONOMICHE ED AZIENDALI
"M. FANNO"**

**CORSO DI LAUREA MAGISTRALE / SPECIALISTICA IN
BUSINESS ADMINISTRATION**

TESI DI LAUREA

**INTERNAL AUDITING: A COMPARISON BETWEEN THEORY AND
PRACTICAL APPLICATIONS THROUGH AN EMPIRICAL RESEARCH**

RELATORE:

CH.MO PROF. FILIPPO ZAGAGNIN

LAUREANDO/A: FRANCESCO BIZZOTTO

MATRICOLA N. 1106200

ANNO ACCADEMICO 2016 – 2017

Il candidato dichiara che il presente lavoro è originale e non è già stato sottoposto, in tutto o in parte, per il conseguimento di un titolo accademico in altre Università italiane o straniere.

Il candidato dichiara altresì che tutti i materiali utilizzati durante la preparazione dell'elaborato sono stati indicati nel testo e nella sezione "Riferimenti bibliografici" e che le eventuali citazioni testuali sono individuabili attraverso l'esplicito richiamo alla pubblicazione originale.

Firma dello studente

I would like to thank my supervisor for the advices and the support provided me during this writing period.

I would also like to thank all the internal auditors and the people interviewed that have dedicated me their time answering to my questions with kindness and generosity.

Finally, I thank my family, Franco, Piera and Francesca, and all my friends for supporting me during hard times.

INDEX OF CONTENTS

Chapter 1: Corporate governance	3
1.1 History of corporate governance.....	4
1.2 Corporate governance frameworks in U.K. and Italy	9
1.2.1 United Kingdom’s theoretical model.....	11
1.2.2 Italy’s theoretical model.....	17
1.3 Criticisms	23
Chapter 2: Risk management	25
2.1 The evolution of risk management.....	27
2.2 The C.O.S.O. Report.....	28
Chapter 3: Internal Controls.....	39
3.1 Definition	39
3.2 Actors involved	41
3.3 Internal controls characteristics.....	43
Chapter 4: Internal auditing	45
4.1 Audit history and today’s spread of the function.....	45
4.2 Definition	47
4.3 What standards requires a C.A.E. to do	49
4.4 Audit approaches.....	52
4.5 Audit field work	54
Chapter 5: Empirical research	67
5.1 The survey.....	67
5.2 General description of the Internal audit function	68
5.3 Positioning of the Internal audit function and relationships with other bodies.....	72
5.4 Audit plan and audit techniques	78
5.5 Management relationships.....	85
5.6 Internal control framework.....	87
5.7 Risk management system.....	88
Chapter 6: The Italian Space Agency Experience	91
6.1 The independent performance assessment body.....	91
6.2 The I.S.A. case.....	92
Conclusions.....	95
Appendix A	99
Bibliography.....	107

Introduction

Companies worldwide face a daily struggle to reach their objectives. Beside profit, that is the reward for the entrepreneurial activity, many others are pursued:

- Being in compliance with the laws and regulations ruling the market the companies are embedded;
- Issuing clear and transparent financial information, in order to give the stakeholders a solid picture of the economic and financial situation of the company;
- Being effective and efficient in running the business.

Internal Audit function has evolved inside companies and more in general into organizations to help reaching these objectives. It has had a huge boost in the last two decades after major crisis and bankruptcies of big companies in the North American scenario happened. Under such circumstances, it seems a really promising function for any organization, and this work will try to demonstrate this thesis. To do so, internal audit function in companies with the headquarter in the North-East of Italy will be investigated. Since in the national scenario internal auditing is strongly advised by the regulation only for companies listed in the stock exchange, these companies will be used as a target for both the theory present in the academic literature and for the empiric part of this work.

To study internal auditor's activities, this thesis will focus on the main audit techniques adopted by the internal auditors and which methods they commonly use in order to help a company to reach its objectives.

The research has been carried out with data collected via surveys sent to a sample of internal auditors that kindly accepted to contribute with their answers, and some of them also agreed with the author an interview.

In conclusion, it will be also presented a case of internal audit applied in a state-owned company, the Italian Space Agency (I.S.A.). A comparison between such a peculiar form of internal audit present in this organization and the general framework valid for public companies will provide additional elements to draw conclusions about a possible future expansion of internal audit in public entities

The work is organized as follows.

Chapter 1 analyzes corporate governance frameworks to understand where the internal auditor is positioned inside a company.

Chapter 2 focuses on risk management, since the internal auditor must determine if the company is facing a risk not to achieve an objective.

Chapter 3 illustrates what internal controls are, since they are the main instruments a company has to deal with risks, and they must be assessed periodically by the internal auditor.

Chapter 4 describes what internal audit is and what an internal auditor does, starting from the history, through the definition, and finally reaching to the techniques that are presented into the most recent literature.

Chapter 5 explains the methodology to collect the data, the sample composition and the data analysis.

Chapter 6 compares what have been learned for internal audit functions with the activities done by a similar body present in the I.S.A.

The conclusions close this work, dealing principally with the main techniques used by the internal auditors and the relations they are able to establish with managers; intervention proposal has been issued in order to enhance the most critical aspects of the role of internal auditor.

Chapter 1: Corporate governance

The definition of corporate governance is not perfectly consistent among the different sources that can be found in the academic literature, and can actually vary widely. Some are shorter and easier, as the one given by the Committee on the Financial Aspects of Corporate Governance (1992 p. 14): “corporate governance is the system by which companies are directed and controlled”. The International Auditing and Assurance Board (IAASB, 2015), instead, defines it as: “the role of person(s) or organization(s) with responsibility for overseeing the strategic decision of the entity and obligations related to the accountability of the entity”. The work of Zattoni (2015) presents corporate governance in a more complex way, saying that it must be present in all companies, except the smallest ones, and that it is a system of mechanisms and processes that work jointly to achieve what’s good for the company: positive economic results and the survival and autonomy in the long run. The paper of La Porta et al. (1999) defines it as: “a set of mechanisms through which outside investors protect themselves against expropriation by the insiders”; the insiders here referred are managers and controlling shareholders.

Corporate governance is also defined by Demartini, Graziani and Monni (2012) as the investigation about the institutional framework organizations adopt to govern themselves. This framework is composed of:

- The stakeholders;
- The contribution that the stakeholders are capable to transfer into the organization, in term of capitals and skills;
- Rewards for the contribution given as dividends or retribution;
- The right to govern the company;
- Mechanisms and structures that regulates the link between contribution and rewards and the way the company is governed.

The etymology of the term suggests that corporate governance means the government of one body as a whole:

- Corporate: means “united into one body” from Latin *corporatus*, past principle of *corporare* “to form into one body”, from *corpus* “body”;
- Governance: means “act or manner of governing”, from French *governance* “government, administration; (rule of) conduct”;¹

¹ Source: www.etymonline.com

A brief review of the history of corporate governance may help to carve out a more comprehensive definition.

1.1 History of corporate governance

In this work, it is presented a brief background of the major circumstances that affected corporate governance's evolution.

The history of the term goes back to the 1976, in the United States.

After World War II, U.S. companies lived a period of rapid growth, but the attention about governance didn't grow as fast. Public companies' board of directors was considered just "collegial and supportive of management" (Cheffins, 2012, p. 2), and a major role was fulfilled by managers, as Pound suggested in 1995 (see Cheffins, 2012, p. 2). Only in case of corporate crisis there was a relevant intervention by the board of directors; this was justified by the fact that the top management was strongly influencing the appointment of the directors.

In the mid-1970s, the Security and Exchange Commission (S.E.C.) discovered a pervasive habitude among the U.S. public companies; many of them were involved in unjustified payments to foreign officials, falsification of corporate accounting and misrepresentations of documents issued. The S.E.C. denounced those methods publicly in a document titled *Report of the securities and exchange commission on questionable and illegal corporate payments and practices*, dated 1976. To solve the problem, they mention a "new governance concept that the Commission ... [is] attempting to instill and its legislative and other proposals are designed to enhance" (S.E.C. 1976, p. 56). In 1977 Harold Williams, chairman of the S.E.C., had a clear design of the ideal board: only the Chief Executive Officer would have been appointed, with the presence of an audit committee, a nomination committee and a compensation committee. He purposed this solution and asked to public companies to reform their system in a voluntary basis (Wright, Siegel, Keasey, 2013). In 1978 Senator Howard Metzenbaum purposed a blue-ribbon recognition to the public companies with corporate governance composed of consumers, shareholders and industry representatives, but this initiative never took off (Wright, Siegel, Keasey, 2013). Two years later, in 1980, he submitted to the Congress the *Protection of the Shareholder's Right Act*, that was requiring to the large public companies to keep independent the majority of the board members, to establish the committees proposed by the S.E.C. in 1977, with the exclusion of the compensation committee, and to give more rights to the shareholders (Congressional research service, no date).

The academics were trying to tackle the problem too. Nader, Green and Seligman were probably the ones that forged the term corporate governance in 1976 in their book *Taming the Giant* (Cheffins, 2012). They proposed a corporate governance scheme very similar to the one we see nowadays.

In 1978 the American Law Institute (A.L.I.) undertook a project on corporate governance, culminated in 1980 with a conference together with the New York Stock Exchange (N.Y.S.E.) and senior corporate executives to discuss new frameworks; the business environment was in favor of the path started, and considered this as an occasion to find a non-governmental solution to the problems appeared in the mid-1970s (Cheffins, 2012).

The fervor revolving around corporate governance had a sudden stop in the early 1980s. From the institutional side, the election of Reagan exemplifying a political shift to the right meant also the change of the S.E.C. chairman. This stopped the majority of the progresses done for the corporate governance cause. In the Congress, the Protection of Shareholder's Rights Act stalled. From the academic's side, the agency cost theorized by Eugene Fama in the 1980 gave to the corporate governance's opponents the input to say that market limitations were sufficient to limit the managerial discretion, and that no further control was necessary. These changes influenced also the progresses made by the A.L.I.; the document about corporate governance that the A.L.I. issued after more than ten years of efforts in 1992, "*Principles of Corporate Governance: Analysis and Recommendations*", contained provisions strongly resembling the existing laws. The results of this work brought no tangible contribution to the corporate governance framework (Cheffins, 2012).

During this decade, other participants joined the discussion that was taking place in the U.S. Institutional investors were continuing to acquire big stakes of public companies shares; to protect their investments they were interested in gaining more and more assurance. In 1984, Jesse Unruh, the state treasurer of California and board member of California Public Employees' Retirement System (CalPERS) had the idea to launch and lead the Council of Institutional Investors (C.I.I.), mainly composed by public pension funds, with the explicit function to lobby for shareholders right (Cheffins, 2012). In particular, this initiative started after the discovery of an illegal practice diffused among the big public companies: in the case of poor financial results and sensing a takeover, managers were trying to resist by using corporate funds to pay great sums to the acquiring company in order to delay or stop the acquisition and maintaining their position (Cal.P.E.R.S., 2015).

From the early 1990s, the C.I.I. started to harshly influence corporate managers, asking to the public companies to invest in transparency and to remove underperforming CEOs from the board. Some of the biggest companies, e.g. IBM, Kodak, General Motors, American Express, complied (Wayne, 1994). Even with those achievements, in almost the totality of the cases the institutional investors

represented only a minority of a company shareholders, and were the only category of investors reasoning with a hands-on logic (Cheffins, 2012).

The corporate governance discussion soon expanded offshore and the United Kingdom was the first country after U.S. to develop an interest in this theme. In 1991, the London Stock Exchange and the Financial Reporting Council created the Committee on the Financial Aspects of Corporate Governance, with the specific objective of creating a set of rules on corporate governance for the British companies. After 18 months, the Committee issued the very first report about corporate governance, known worldwide as the *Cadbury report* from the chairman of the committee, Sir Adrian Cadbury. This report gained attention in the U.K.'s business world and abroad; due to some severe cases of financial scandals, the business and institutional worlds of the developed countries were gaining interest in corporate governance. Cadbury introduce the work of its commission with the following words: "The harsh economic climate is partly responsible, since it has exposed company reports and accounts to unusually close scrutiny. It is, however, the continuing concern about standards of financial reporting and accountability, heightened by BCCI², Maxwell and the controversy over directors' pay, which has kept corporate governance in the public eye" (Cadbury report, see Committee on the Financial Aspects of Corporate Governance, 1992, p. 8). After the publication of this report, London Stock Exchange obliged listed companies to follow the *comply or explain* principle; companies would have to fully comply with the rules of the Cadbury report or explain why they didn't do so.

The Cadbury report collects the majority of the best practices still present in the modern principles of corporate governance. It has been updated every three years by the Committee on the Financial Aspects of Corporate Governance: in 1995 by the *Greenbury Report* and in 1998 by the *Hampel Report*. June 1998 saw the consolidation of the three codes in a publication known as the *Combined Code*. Since 1998 it has been updated many times by the Financial Reporting Council, and is still setting corporate governance' best practices nowadays. It is also known as "the Code" in the U.K. After those events, the Organization for Economic Co-operation and Development (O.E.C.D.)³ was asked by the member countries to establish a set of principles, intended to be guidelines to improve all the domestic legal, institutional and regulatory frameworks. Those principles were based on the experience developed by the member states and big institutions as World Bank and Monetary Fund (O.E.C.D., 1999). O.E.C.D. published his principles in 1999.

² Bank of Credit and Commerce International, one of the biggest organizations that went bankrupt in the early '90s.

³ O.E.C.D. is an organization born in 1961 to achieve: economic growth, employment, financial stability, expansion of trade among the member states. It is composed mainly by European and North American countries.

Italy didn't participate to the global corporate governance brainstorming but followed the main current in the late 1990s. In 1998 the legislative decree N. 58, better known as the consolidated law on finance, laid the foundations for the creation of an Italian *corporate governance code* aligned with the U.K. codes. The following year Stefano Preda, chairman of Borsa Italiana S.p.A., the main stock exchange in Italy, decided to create and preside over a commission dedicated to the creation of the first Italian *corporate governance code*. The Italian experience followed the U.K. model: a proactive movement promoted by the stock exchange to achieve efficiency and dependability in order to develop more competitive companies and to attract more capitals. (Preda Code, see: Comitato per la corporate governance delle società quotate, 1999). Preda strongly wanted a mixed composition for the committee; a quote of academics, but also presidents and CEOs of major Italian listed firms. This gave to the newborn code a self-regulatory nature, in order to be seen not as an additional imposition or request by the stock exchange firm, but as a concrete possibility of improvement. The code reflected the best practices present in the U.K. codes and coming from the U.S. and adapted them to the Italian corporate scenario, characterized by massive ownership concentration, usually in the hands of "industrial families" (Drago, C., et al., 2011), with the risk of controlling shareholders dominating over minority shareholders.

The process to introduce some corporate governance elements started very gradually; Milan stock exchange decided not to introduce immediately the above described *comply or explain* principle, but instead it asked to listed companies to comply voluntarily if they recognized a tangible benefit from the adoption.

In 2001 the legislative decree N. 231 enlarged the corporate governance regulation, introducing a commission monitoring the responsibilities of the board or managers for the commission of crimes caused by an inadequate organization of the governance⁴. Two years later with the Vietti reform, legislative decree N. 6 of 2003, the Italian legislator offered to the companies the possibility to adopt different corporate governance schemes by introducing into the civil code:

- The one-tier system is characterized by shareholders' meeting appointing a board of directors, which in turn appoints, from its members, the supervisory body.
- The two-tier system is characterized by the shareholders' meeting, appointing the supervisory body, which in turn designate the corporate body responsible for the management of the company.

⁴ Organismo Di Vigilanza (O.D.V.) is the Italian original name.

Public companies, however, seemed unenthusiastic about those possibilities: in 2014, eleven years after the reform, only 2% of them transitioned to one of the new schemes available (De Molli, V., Visani, M. 2015).

During the first half of 2000s Italy witnessed a succession of financial scandals, e.g. Parmalat and Cirio, that enlarged the series of other global severe bankruptcies happened worldwide in those years; the major were in 2002 in the U.S., that suffered for the default of Enron and Worldcom, both triggered by the illegal accounting practices not discovered also in consequence of the weaknesses diffused in corporate governance system and culture.

As in the U.S. the Congress reacted quickly to those scandals with the Sarbanes-Oxley Act of 2002 (Roman, R. 2004), the Italian events originated in 2005 the Law N. 262 (Drago, C. et al. 2011), better known as the law on savings. The main purposes were to add protection schemes to shareholders and substantial features to Italian corporate governance.

In conclusion, we saw how corporate governance was thought as a solution to the problem of separation of property from governance. Here, a problem rises; in the U.S., this separation is embedded in a general situation where there is a wide fragmentation of shareholders with little power over the governance, that makes easy for the management to act egoistically and not for the interest of the shareholders if the board is not careful. In Italian companies, instead, a different problem worries the investors. Corporate governance is often developed to contrast the overpower of majority shareholders that can dominate minority shareholders. (Enriques, L., Volpin, P., 2007). For both the problems the solution is to give assurance to the shareholders that the company is conducted well, that a solid control system is in place and that all the risks that could rise are individuated and managed to a bearable level. The internal audit function plays a crucial role in all those activities.

Below is shown in figure 1.1 a timeline that exhibits the main milestones of corporate governance.

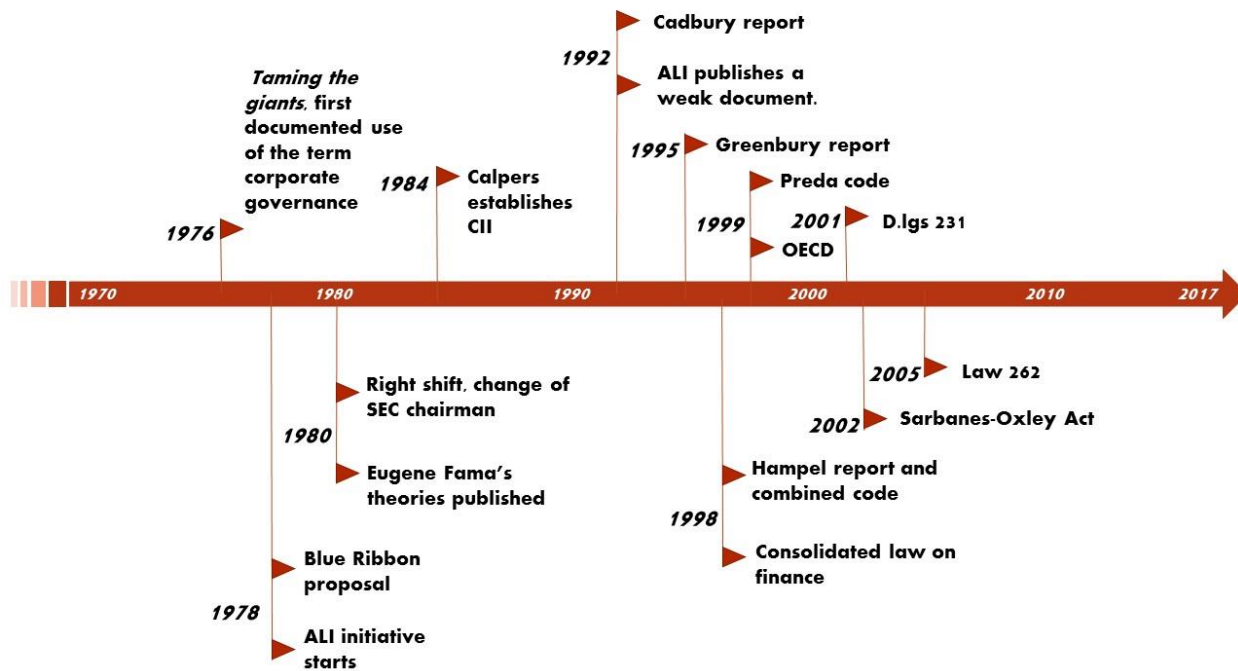


Figure 1.1: Corporate Governance timeline.

1.2 Corporate governance frameworks in U.K. and Italy

In the first paragraph, it has been shown how modern corporate governance originated from the combination of opinions and ideas proposed by different economic operators, coming from different background and extractions, with the scope to safeguard their interests. In many cases those ideas were originated from investors worried about the separation between control and ownership and have been later endorsed by the legislator.

It will now be analyzed the outcome of the evolution of the corporate governance for public companies. To do so, this work will compare the current Italian corporate governance framework with the one applying in the United Kingdom; this comparison can be considered robust given the similar structure of the legal framework ruling over the corporate governance. This similarity is no surprise, since the Italian framework originated mainly from the U.K.'s one, more specifically from the Cadbury report and following.

It is ascertained that the first Italian laws and documents about corporate governance were built up following the example and the general structure coming from the Anglo-Saxon experience. In particular, Enriques and Volpin (2007, p. 138), referring to the corporate governance systems of France, Germany and Italy, state that: “a good part of the European reforms has been patterned after U.S. corporate and securities law”, especially taking inspiration from the Sarbanes-Oxley act of 2002.

The shape in which the Italian system evolved resemble instead majorly the regulations present in the U.K. In this latter country and in Italy, the corporate governance scheme is based on two sources of law: primary laws emitted by the legislator and secondary laws published by commissions or authorities empowered by the primary laws. The secondary laws are extremely important for the purposes of corporate governance for the presence of a code that lists all the best practices that will allow a general company to be compliant with the law and efficient.

In Italy, as primary laws are represented by the legislative decree N. 58/1998, emitted by the legislator. The secondary laws, instead, are published by commission or authorities empowered by the primary laws. In this category can be found the Italian *corporate governance code*, issued for the first time in 1999 and subsequently updated several times. As Alvaro, Ciccaglioni and Siciliano (2013) affirm, this code was useful to anticipate and experiment some paths that would subsequently converted into laws, to receipt EU Commission's recommendations and, in some cases, to clarify what present laws were requiring to the companies. Today, the adoption of the provisions present in the corporate governance code is voluntary, but in case of departure from the recommendations the issuer must explain the reasons for the choice. The *comply or explain* principle has been copied in Italy from the U.K. experience as a significant method to not underestimate the code. Coombes and Wong (2004) assert that this principle force the companies to ponder well any deviation from the code. If justified, the deviation can be transparently explained to all the stakeholders and the media. This allows for flexibility among the companies. It is commonly accepted that the rule *one size fits all* can create inefficiencies, especially for companies with sizes far from the mean or participating in difficult markets. At the same time, the *comply or explain* principle punishes the unjustified deviation from the provision: uncommon decisions would probably be carefully examined by media or watchful shareholders that will trigger protests.

The next paragraph will present the theoretical corporate governance framework presented by Pickett (2010), based on the U.K. regulation and mostly taken from the pioneering work of Cadbury, dated 1992. Successively it will be compared to the Italian framework for corporate governance, referring only to the traditional system and not considering the rarely-used one-tire and two-tire systems. As first thing to understand the two frameworks, the bodies and actors composing the model must be presented. Successively the focus will be shifted on the relationship existing between the internal auditor and the other corporate bodies and on the role of the different bodies into the internal control and risk management system. Only provisions for public companies will be taken into consideration, which apply to the typology of organization composing the sample studied in the empirical part of this work.

The frameworks are composed by the provisions contained into the above-mentioned codes and providing the standards for corporate governance into the two countries, backed and legitimized by primary laws.

1.2.1 United Kingdom's theoretical model

Shareholders

At the top of the model can be found the shareholders; their role is well described in the Cadbury Report (Committee on the financial aspects of corporate governance, 1992, p. 14): “to appoint the directors and the auditors and to satisfy themselves that an appropriate governance structure is in place”. In return for their investment, they have the expectation to receive dividends, the return on capital provided, or at least not to see an impairment of the assets value.

The U.K. provisions do not let the possibility to the minority shareholders to appoint directors to the board. The mechanism through which they are safeguarded is the presence of independent, non-executive directors that should ensure that the interests of all shareholders are considered in making strategic decisions.

The board of directors

The board of directors is the body responsible for the governance of a company. Even if it has a chairman and three sub-committees, it is collectively responsible for the long-term success of the company. It is composed of executive directors and non-executive independent directors and the latter should compose at least half of the board. The independent directors are those members of the board that meet the independence criteria⁵ listed in the Code, that certifies that there are not “circumstances which are likely to affect [...] the director's judgement” (Financial reporting council, 2016. p. 10). The independence of a director is established through an assessment made by whole board of directors. The total number of members of the board is variable.

The main tasks it is in charge for are:

- Setting the long-term strategy and the objectives of the company;
- Establishing the culture, values and ethics of the company;
- Determining the nature and extent of principal risks it must take to achieve the objectives and how they have been managed and mitigated;

⁵ For further information, see (Financial Reporting Council, 2016. p. 10)

- Setting internal control system and risk management system and assessing it at least annually, with the help of the other competent bodies;
- Appointing the top managers and monitoring their conduct;
- Supervising the management;
- Writing an annual report to the shareholders with the inclusion of the mechanisms through which the board operates, which are the decisions are taken by the board and which by the management;
- Choosing the senior independent director among the independent directors;
- Explaining in the annual report the business model of the company and their responsibilities with respect to the preparation of the report itself and accounts;
- Establish an audit committee, composed of at least three independent non-executive directors, and at least one member has relevant financial experience.

To achieve those responsibilities, the board will be more effective if it meets some conditions. It should:

- Be composed of people differentiated by gender, race, skills, experience, knowledge and independence;
- Achieve a clear division of responsibilities;
- Discuss each issue, and there shouldn't be any member able to take unfettered decisions;
- Equip itself with formal, rigorous and transparent procedures for the appointment of new directors, with the help of the designated committee;
- Encourage the continuous formation of its members, to update skills and knowledge, especially for boards of companies present in fast-changing markets;
- Be constantly fed with good quality information from the various level and bodies of the company;
- Keep a formal, annual process to evaluate its performance and that of its committees and individual directors;
- Have a part of its remuneration linked to the long-term success of the company; every performance-related element should be transparent and clear and no director should be involved into the process of deciding his own remuneration;
- Pass through a formal and rigorous process of evaluation of each member's and of each commission's performances annually.

Chairman of the board

The chairman of the board should not be the C.E.O.⁶ of the company, and should meet the independence criteria.

He has the leadership of the board, sets the agenda, promotes the respect of main company's principles and ensures that sufficient information is given to each director and to each committee to conduct their tasks.

The chairman is responsible for the promotion of openness and objective-aimed debate inside the board. He should promote the engagement of the non-executives into the debates. To avoid information biased that could grow inside a board, the chairman should meet schedule meeting of the board without the presence of the executive directors. The chairman should also encourage the continuous formation of the members of the board and make sure that the new directors receive a satisfactory introduction as they join the board.

Non-executive directors

As Roberts, McNulty and Stiles (2005, p. 1) states: "non-executives can both support the executives in their leadership of the business and monitor and control executive conduct". They should not be only a supervisory part of the board. To analyze the performance of the management, the integrity of financial information and to set the remuneration of the directors is a narrow job definition for them. Instead, they should be also contributing to the decision of the strategic aims of the company. The non-executive directors could meet the criteria to be considered independent or not. For those with independency status, they have a role into appointing and removing executive directors. Among the independent directors a senior independent director should be chosen, serving as an intermediary between the chairman and the other non-executive directors or between the chairman and the shareholders in the cases in which other communication channels are not providing a fast response. The senior independent director should meet at least annually with the other non-executive directors but without the chairman of the board to discuss his or her performances.

Audit committee

The audit committee must be endowed with competence in the sector the company is involved. It is composed by three independent non-executive directors.

It has to:

- Monitor the robustness of the financial statements and reports;

⁶ Chief Executive Officer.

- Review internal controls and risk management system;
- Monitor and assess the performances of the internal audit function;
- Advise the board and the shareholders in the process of choice or removal of the external auditors and reviewing the effectiveness of the audit process;
- Implement policies on the supply of non-audit services⁷.

Nomination committee

The nomination committee is in charge of finding new potential directors and suggest them for being appointed. The committee also evaluates the composition of the board of directors and suggests new members mainly to equilibrate skills, experience, independence.

Remuneration committee

The remuneration committee has the role of deciding the remuneration of the executive directors, of the chairman and of the top management. The remuneration should be designed to be attractive for the people with the necessary experience and skills for the office, but also conceived considering the long-term success of the company. If part of the remuneration of the executives is linked to the accomplishment of some objectives, the criteria must be clear and transparent.

External auditors

The external auditors are present in the corporate governance framework to increase the confidence level of the users of a company's financial statements. To do so, the auditor must express an opinion on: "whether the financial statements are prepared, in all material respects, in accordance with an applicable financial reporting framework" (International Auditing and Assurance Standards Board, 2015). To form the opinion, the auditors must deeply analyze the internal controls and the processes of the client's company to understand if the financial statements are free from material misstatements due to fraud or errors.

Internal auditors

The internal audit function is led by the Chief Audit Executive (C.A.E.) and composed by other internal auditors depending on the company's dimension. This function is fundamental for the achievement of the three main objectives: compliance with the law, transparent information flowing inside and outside the company and operational efficiency. In the opinion of the Institute of Internal

⁷ Counseling services provided by external audit firms.

Auditors (2016 p.12), “The internal audit activity must assess and make appropriate recommendations to improve the organization’s governance processes for:

- Making strategic and operational decisions;
- Overseeing risk management and control;
- Promoting appropriate ethics and values within the organization;
- Ensuring effective organizational performance management and accountability;
- Communicating risk and control information to appropriate areas of the organization;
- Coordinating the activities of, and communicating information among, the board, external and internal auditors, other assurance providers, and management”.

Hierarchically, the internal audit function depends directly from the board of directors or the audit committee. Since internal auditors have also to oversee management’s work, this provision ensures that the independence characteristics of the function is preserved and that information reaches the board without any type of interference.

The internal audit function works in strict contact with the audit committee, that approves its audit plan, require periodical reports and evaluate its work.

British legislator insists for the presence of an internal audit function in listed companies that are currently without it by asking to the audit committee to review annually the possibility of its institution.

Management and other personnel

The role of managers and all the human resources of a company in the corporate governance scheme could be perceived as marginal. However, this vision is way too trivializing. All the personnel should be informed of the main characteristics of the company’s corporate governance framework and aware of their role and responsibilities in it.

Managers, in particular, have a crucial role in internal controls: they are required to design controls for the function they are directing.

Employees have to carefully apply those controls.

After having briefly presented the participants to the corporate governance framework in the U.K., below is explained the way it works. The whole framework is then summarized in Figure 1.2.

The U.K. theoretical model

The top of this corporate governance framework is reserved to the shareholders. They are the ones interested in a good governance as a protection scheme for their investment in the company's equity. The shareholders choose and appoint the board that will set the strategic aims to conduct the company to the maximization of its value. To conduct the day-by-day operations the board employs the managers and all the employees needed to achieve the objectives. The role of the board includes also the control over the performances of the management. To control and steer their work, the board sets targets, approves a budget for each manager and establishes a method to measure their performances. Stakeholders need to receive formal and standardized information from the company about the integrity of the equity (and thus of their investment) and if there is ground for receiving dividends. The shareholders require accountability to the board. To allow the creation of all those information, all relationships with the third parties are recorded in the accounting system, that will produce two fundamental documents: the balance sheet and income statement.

The final accounting documents are then checked by the external auditors, that will form their opinion to enhance the confidence of the shareholders. The audit committee has the role to maintain the relationship with the external auditor and is assisted by the internal auditors.

The internal audit function has not only this point of contact with other bodies inside the corporate governance framework. It is well defined by Allegrini (2011) as the board of directors's right hand; it is a fundamental function that has a deep understanding of internal controls and of risk management, and can use it to advise both the board, the audit committee and the management. A good relationship between the internal auditors and the audit committee helps boosting the quality of internal controls and risk management (Pickett, 2010). It is also a crucial function for the external auditors to deal with, in order to understand if the controls in place are robust enough to provide a barrier to fraud and errors.

The other two board committees are a solution found by the authors of the Code to enhance the confidence of the investors in the skills, experience and results obtained by the board.

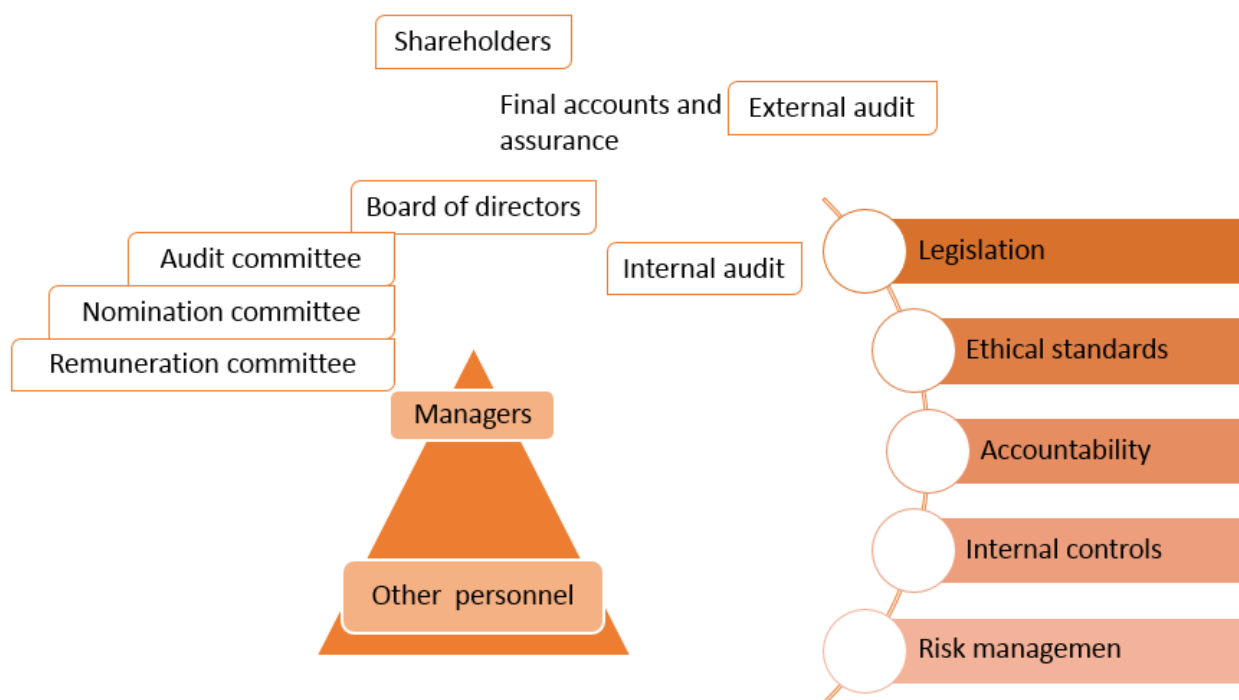


Figure 1.2: the U.K. corporate governance model. Inspired by Pickett, 2010.

1.2.2 Italy's theoretical model

Italian's corporate governance scheme has some differences from the British one. In this part, only the bodies with major discrepancies or not present in the U.K.'s provisions will be presented. The information regarding the Italian theoretical model will be based not only on the *corporate governance code* (Corporate governance committee, 2015) provisions, but also on the summarizing work of La Manno (2012).

The shareholders

The shareholders appoint the board of directors during the shareholders meeting. A major difference is present in the fact that minority shareholders have the possibility to appoint one director, with the function of ensuring that the interests of every shareholders is taken in consideration by the whole board of directors. The reason for this provision lays in the composition of the shareholders of many Italian companies, with very concentrated property that could potentially dominate over the minority shareholders.

The shareholders appoint also a member of the board of statutory auditors. With the advice of this body, the shareholders meeting appoints the external audit firm.

The board of directors

The role of the board of directors and its chairman are almost identical to those already seen for the British framework. It is important to remind that it provides the strategic guidance to the company, appoints the top management and report to the shareholders its functioning and the results obtained. For Enriques and Volpin (2007), an important role of the board is the screening of the related party transactions, i.e. operation among the company and third parties that could create situations of conflict of interests dangerous for the interests of the shareholders.

The fact that at least one third of the directors must meet the independence criteria listed in the Italian *corporate governance code* and the presence of the director appointed by the minority shareholders ensure a wider representation of the shareholders and that all the different interests are kept in consideration. The U.K. office called senior non-executive director has a similar counterpart in the Italy, called the lead independent director, with almost identical tasks.

The board must designate one of its members deemed in possess of adequate risk management and control competences as responsible for internal control and risk management. In addition to this office, the board creates three committees composed of at least three non-executive independent directors.

The companies included into the FTSE-MIB⁸ may consider the creation of a fourth committee in charge with the supervision of sustainability issues.

The board of directors appoints the internal auditor and approves the annual audit plan.

Remuneration committee

The remuneration committee has a role very similar to the one already explained for the U.K.'s model.

Nomination committee

The role of this committee is to find new directors that could enrich the composition of the board. In the choice of the new directors, the committee should keep into consideration the interest of the minority shareholders.

Control and risk committee

It is a committee present only in the Italian framework, supportive of the board of directors in the definition and evaluation of the internal control and risk management system. At least one of the components must have experience in accounting and finance or risk management.

Precisely, the tasks of this committee are:

⁸ The 40 biggest companies with the largest capitalization.

- To evaluate the correct application of the accounting principles;
- To express an opinion regarding the identification of the main corporate risks;
- To review the periodic reports of the internal auditor over the internal control and risk management system;
- To monitor the independence and the performances of the internal auditor;
- To request to the internal auditor to investigate over specific operational areas.

The Board of Statutory Auditors

This body is required by the legislator through the article 2403 of the Italian civil code and represents the link between the supervisory system of a company and the investors. The statutory auditors must oversee the compliance with the legal framework and with the company's by-laws. In addition, it assesses the adequacy of the organizational, administrative and accounting structure of the company (Abriani, Clavosa and Ferri et al. 2012). The board is composed of three independent members; this characteristic ensures to the minority shareholders that their interests will be always taken into consideration, even if it is the majority of the shareholders that appoints the statutory auditors. The fact that the chairman of the board of statutory auditor is chosen by the minority shareholders adds an element of impartiality.

The board of statutory auditor is at the top of the internal control system, must receive reports and information in case of issue with the system on internal controls from the internal audit function and disclose an opinion about the appointment of its members to the board of directors. The board of statutory auditor could also be entrusted with the tasks required by the Legislative Decree N. 231 of 2001, regarding the surveillance over crimes committed by a company.

Following the disposition of the Legislative Decree N. 39 of 2010, in the event of the choice of the new external audit firm the board of statutory auditors purposes a candidate.

Person responsible for the preparation of the corporate financial documents

To enhance the transparency of the information flowing from the company, the legislator introduced in our legal framework this figure with the Law N. 262 of 2005. The companies must appoint a manager which is in charge of controlling that the data flowing from the company to the shareholders is as clear and correct as possible; obviously, in order to do so, the data flowing inside the company must be correct and precise as well. He is responsible for arranging adequate administrative and accounting procedures that will allow the preparation of transparent financial documents. To accomplish his tasks, the person responsible for the preparation of the corporate financial documents often cooperates with the internal auditor.

Director responsible for the internal control and risk management system

This is a role not required by the law but advised in the Italian *corporate governance code* in the provision 7. P. 3. This director is usually the C.E.O., but could also be a non-executive director. He should be a director in possess of the right skills to deal with the system of internal controls and risk management. This director should:

- Maintain an effective internal control system;
- Help the board in the process of identification and management of the company risks;
- Take care that the guidelines issued by the board of directors for the corporate governance are applied;
- Refer to the board any rising issues during the execution of his tasks;
- Support the board in the approbation of the audit plan presented by the internal auditor;
- Be supported by the internal auditors in case of a deep investigation over the internal control and risk management system.

For the sake of simplicity, further on this role will be described as director responsible for risks and controls.

External auditor

The external auditor assurance role is defined by the international principles issued by the International Auditing and Assurance Standards Board (I.A.A.S.B.), applying in Italy as well. The external auditor collaborates with the board of statutory auditors and exchange with this body relevant information.

Internal auditor

The first difference from the U.K.'s *corporate governance code* is the fact that the Italian one refers always to the C.A.E. instead of the internal audit function.

As in the British model, the internal auditor is hierarchically dependent directly form the board, even if significant relationships are maintained with the board of statutory auditors, the person responsible for the preparation of the corporate financial documents, the director responsible for the internal control and risk management system, the external auditor and control and risk committee.

The C.A.E. is defined as the operating arm of the board of statutory auditors or even of the C.F.O., as Allegrini (2011) states. Often it is also member or chairman of a supervisory body introduced in this framework by the legislative decree 231 of 2001, that act as prevention against possible crimes

committed by the company. The inclusion of the C.A.E. into this body is quite common given that the antifraud activities are normally conducted by internal auditors.

The C.A.E. should:

- Verify the functioning of the internal control and risk management system through an audit plan approved by the board of directors;
- Write periodic reports about his activity and about the effectiveness of the methods through which managers intend to mitigate the risks individuated;
- Write reports each time significant events occurs;
- Submit the reports to the board of directors, to the chairman of the statutory auditors and to the control and risk committee;
- Verify the effectiveness of the information system.

A more accurate job description of the C.A.E. will be presented in Chapter 4, solely dedicated to this actor.

Management

The Italian *corporate governance code* requires the management to be in charge of the first and second level control. The first level control is carried out by the operational areas managers, whereas the second level control is entrusted by the business department managers that should identify broader risks as the operational, financial, market, compliance.

As for the U.K. corporate governance framework, below is presented the functioning of the Italian one.

The Italian theoretical model

The shareholders meeting appoints the board of directors, the board of statutory auditor and the external audit firm during the shareholders meeting. The shareholders are entitled by the law to receive correct and transparent financial documentation relating to the results obtained and the main tasks and activities of the board of directors. The board forms the three committees, chooses the director responsible for the internal control and risk management system and appoints the internal auditor. The board appoints also all the top management that has to run the daily operations and should be well aware of its role into the internal control and management system as the first and second line of control. The whole personnel should also be aware of the main characteristics of the

internal control system of the company. Another important role of the board of directors is the publication of the ethical standards that all the people working inside the company must follow.

The nomination committee and the remuneration committee have similar roles to the one already explained for the U.K. model.

The control and risk committee is composed by directors, at least one expert in accounting and finance and, and is the main advisor of the board of directors for all the decisions and guidelines to be issued regarding the internal control and risk management system.

The director responsible for risks and controls is delegated to implement the guidelines issued by the board. The board of statutory auditors has a supervisory role over the company internal control and risk management system, the accounting structure, the by-laws and oversees that the legal framework is respected.

The person responsible for the preparation of the corporate financial documents is responsible for arranging effective administrative and accounting aimed at the preparation of the financial documents.

The internal auditor is a key gear in this mechanism. Its competencies and tasks are the same present in the U.K. model, because taken from the international standards and the best practices. He is considered by the Italian *corporate governance code* as the ultimate (or third) level of control over the corporate risks. The internal auditor's independency and adequacy is assessed by the board of statutory auditor, his audit plan is approved by the board, and he may be asked to conduct inspections over specific areas by the other bodies involved with the internal control and risk management system. The internal auditor produces reports regarding his work and the situation of the system addressed to the main bodies he is in contact with, as above mentioned.

As in the U.K. model the financial statements are controlled by the external auditors, the same applies for the Italian provisions. The external auditors exchange information with the internal auditor to facilitate the respective jobs.

Figure 1.3 summarizes the Italian corporate governance framework.

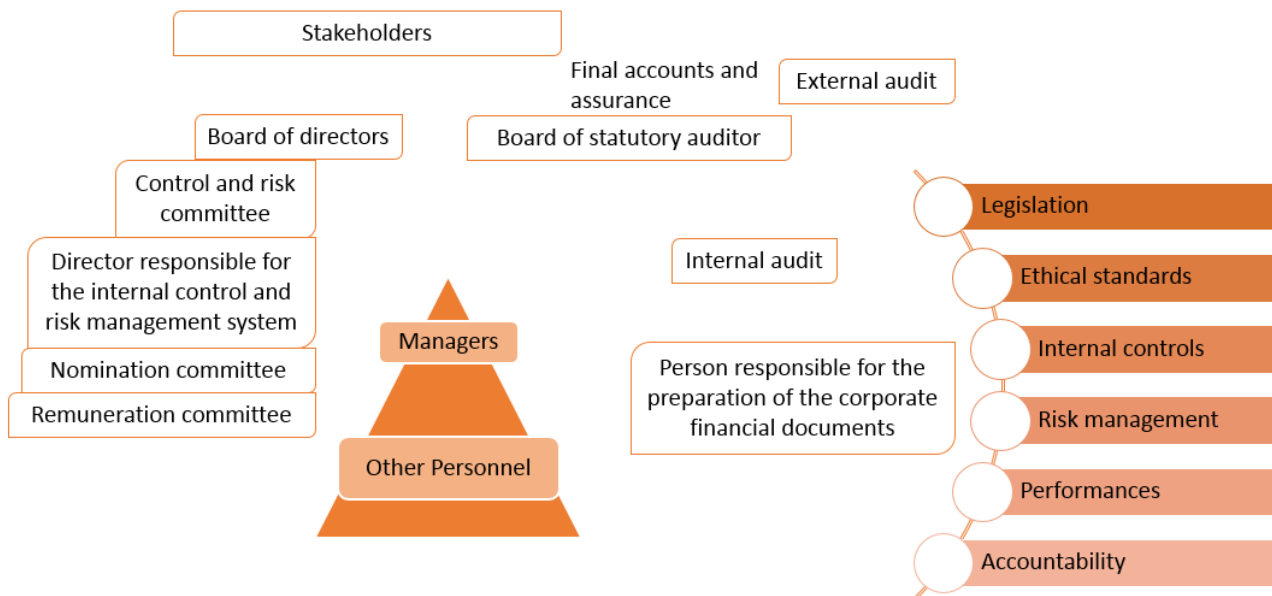


Figure 1.3: the Italian corporate governance model. Inspired by Pickett, (2010) and La Manno (2015)

1.3 Criticisms

There are several critiques directed to the modalities of implementation of the Italian corporate governance framework.

Enriques and Volpin (2007) highlighted that a system should take as a reference another one with similar foundations and legal framework. Instead, the Italian corporate governance framework was built following the international experience that was available in the late 1990s, based mainly over the U.S. and U.K. experience. Those economies are characterized by a structure of the corporate equity in average more dispersed than the Italian one. Corporate governance should allow the legislator to solve those problems: if in the Anglo-Saxon world the shareholders have to defend themselves from managers that could act egoistically, in Italy the minority shareholders fear the power of the majority shareholders, with different interests, that may influence the behavior of managers.

The Italian legislator introduced a number of significant reforms since the Preda Code, dated 1999, and “special emphasis was placed on empowering minority shareholders and on disclosure, which are the most effective tools for countering abuses by dominant shareholders” (Enriques Volpin, 2007). As Bianchi (2010) affirms, the reforms produced many overlapping, especially among the corporate functions with control responsibilities. By learning the functioning of the Italian corporate governance framework, it appears clear how nearly every actor in it have a general controlling role besides its peculiar tasks, creating a quite confusing picture.

Chapter 2: Risk management

As seen in the precedent chapter, the internal auditor is one of the main actors of the corporate governance system. His relevance is due to his prominent role inside the risk management and internal control system.

This chapter will present how is built a risk management system and its importance inside the company environment, with special emphasis on the role of the internal auditor during the designing phase and the day to day management of the system.

To understand what is risk, this chapter start from definitions that describe what companies face in every action or operation done and in each decision taken. Some of the most accurate definitions found come from the two documents setting the standards, respectively, for the internal and the external audit profession.

“Risk: The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood” (The institute of internal auditors, 2013, p. 41).

“Business risk: A risk resulting from significant conditions, events, circumstances, actions or inactions that could adversely affect an entity’s ability to achieve its objectives and execute its strategies, or from the setting of inappropriate objectives and strategies” (International auditing and assurance standard board, 2015, p. 16).

Both definitions link the notion of risk to the achievement of objectives. Indeed risk, from a broad view, represents the uncertainty that a complex and broad series of events could generate an outcome partially or totally unexpected by managers (Renn, 1998). Figure 2.1 represents single risks as little red circles. They are all the possible events that can happen in the near or far future which separate the objective, or desired outcome, from the real outcome.

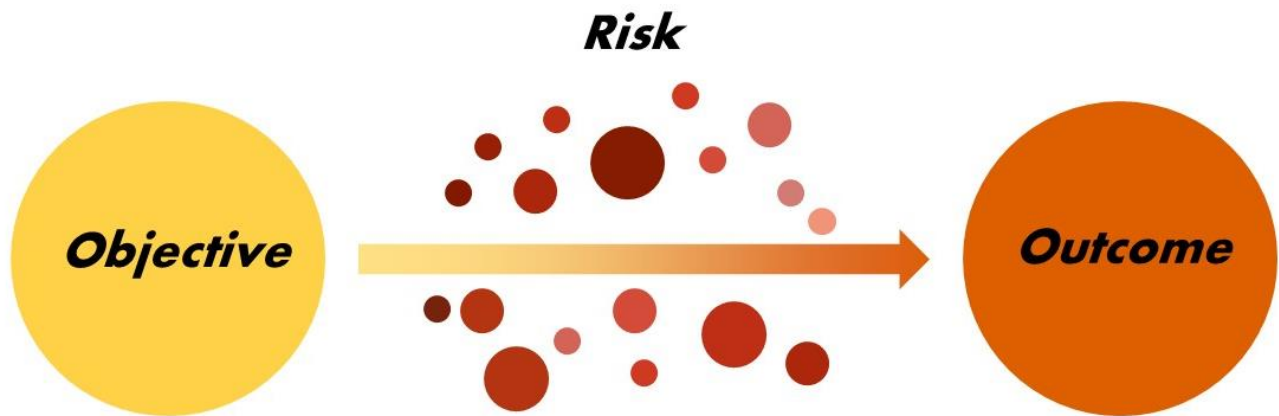


Figure 2.1: How the real outcome is generated from the desired outcome.

The modern definition of risk adopted by many authors do not strictly stick to the link between risk and events damaging a company, like economic losses or security and health problems. Risk should be seen as intrinsically positive or negative but only as an interference with the achievement of an objective. As a consequence, the interference creates two possible outcomes: losses to bear and manage and opportunities to handle and ride.

The association between opportunities and risk may sound faulty and confusing because the link between risk and downsides, or losses, has built overtime since the birth of the word risk; indeed, risk derives from the Spanish word used for reef, *risco*, an obstacle the ships would face to get into the port. However, potentially harmful situations could be generated by apparently positive situations too.

For the sake of clarity, let's imagine a simple case scenario: a sushi factory grows seaweed and raises fish in the waters of a small, controlled lagoon. The increasing temperatures boost the growth of sea weed, and the owners could not be happier for this positive event happened. But this unexpected event may trigger hard times for the owners to harvest all the sea weed in time. A considerable part of the sea weed may decompose and lead to a plummeting of oxygen levels in the water, resulting in the death of all the fishes. This simple example shows how an uncertain and unpredictable positive event generated complexity difficult to manage, and by consequence losses. Reassuring, we may qualitatively divide risk into two categories: positive variations from the expectations (upside risk) or negative variations (down side risk).

Both definitions seen in the previous page describe risk as a probabilistic concept. Following an econometrical approach, we can define the risk as the probability distribution of the possible outcomes around our objective. This approach is described in Figure 2.2⁹.

⁹ The design of the distribution function as a normal (bell-shaped) is for example purpose only.

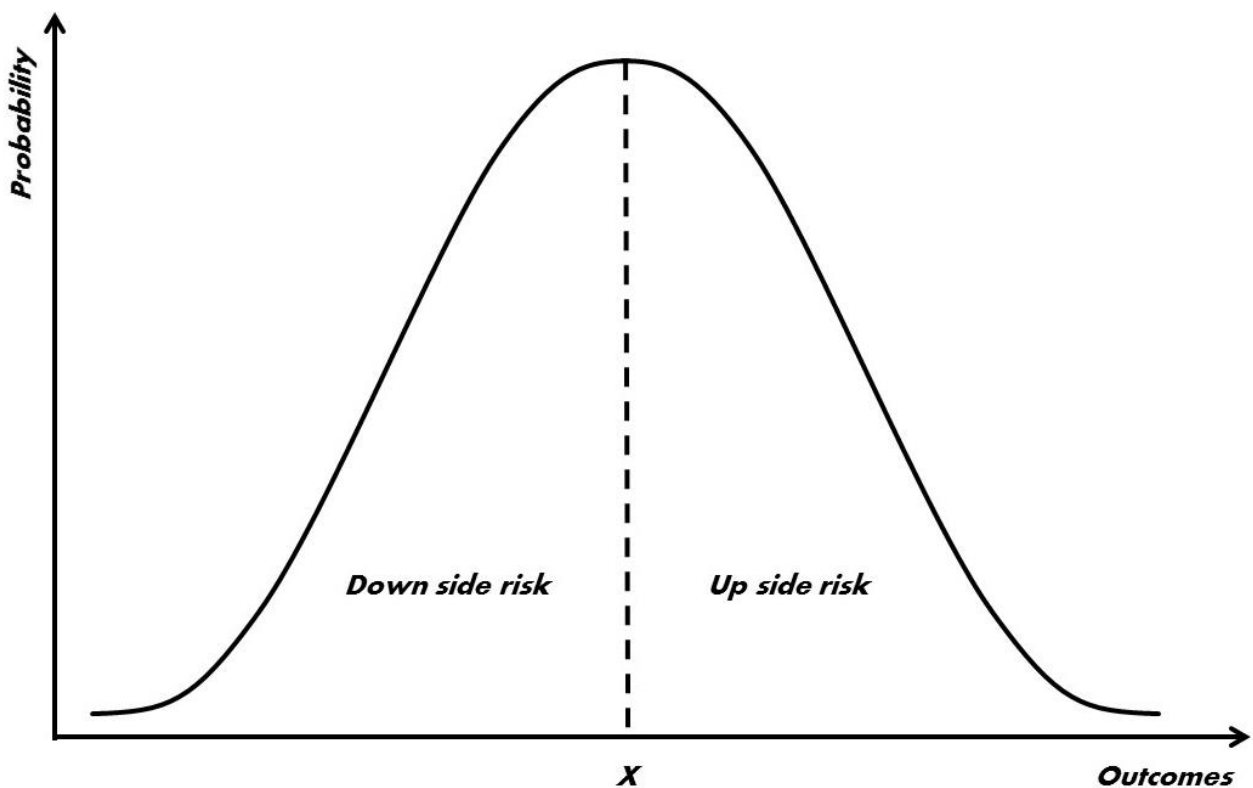


Figure 2.2: risk represented as the probability distribution around the desired outcome X. Liberally inspired from Segatto, 2013, p 21.

Companies' managers and directors encounter risks daily, and they have to adopt a method to organize risk proactively, a framework embedded in the strategic planning that helps to recognize risks, distinguish upside risks from down side risks and providing reports about the ways to catch the first and reduce the latter (Aureli, Ciambotti, Salvatori, 2011).

2.1 The evolution of risk management

The legislators of many countries worldwide accelerated the process of adoption of a framework by big companies. In the U.S., this influence on companies was exerted by the Sarbanes-Oxley Act and the N.Y.S.E. corporate governance rules for listed companies (Paape, Speklè, 2011). For the Italian case, steps in this direction have been taken with the legislative decree 231 of 2001, the Preda Code and the transposition of the U.E. directive 51 of 2003 with the art. 2428 of the Civil Code (Aureli, Ciambotti, Salvatori, 2011).

Risk management frameworks available to companies have been evolving in time. For the sake of completeness, it will now be presented one of first framework adopted by most of the firms in the 1990s and in the early 2000s, and by few companies still today. At that time, risk management was conceived by organizations in “silos” (McShane, Nair, Rustambekov, 2011), and handled at business unit level, each one operating separately and autonomously from the others and led by a unit cost efficiency principle. The silo framework, also known as Traditional Risk Management (T.R.M.), has the major problem to not considered the countless interactions among risks and focuses mostly on the short run objectives, without embedding risk management in a strategic long run view. As many authors agree¹⁰, the lack of coordination between business units and the lack of a holistic view create an economically inefficient risk management. Obviously, one clear advantage is provided by the simplicity of model, that it is easy and straightforward to design and run. This thanks to the fact that managers do not have to calculate the various cross effects among divisions. But big public companies can afford a more refined way to manage risk.

T.R.M. gave the basis to build an innovative framework, that considers the “aggregated risk inherent in different business activities...[and] provide a more objective basis for resource allocation” (Hoyt, Liebenberg, 2011, p. 797). This model is the Enterprise Risk Management (E.R.M.). It spread fast among public companies and nowadays “the idea that E.R.M. is a key component of effective governance has gained widespread acceptance” (Paape, Speklè, 2011p.4).

The success of the E.R.M. theory stimulated the creation of a new figure inside companies: the Chief Risk Officer (C.R.O.), responsible for the risk management system and the identification and assessment of risks. The C.R.O. also advise managers for the best ways to deal with them (Liebenberg, Hoyt, 2003).

2.2 The C.O.S.O. Report

In 2004 the Committee of Sponsoring Organizations of the Treadway Commission (C.O.S.O.¹¹), formalized and issued its E.R.M. framework. The models issued by C.O.S.O. for risk management and for internal controls are true milestones in international corporate governance and are the most used among the bigger public companies, with a coverage rate of 93% in the U.S. in April 2015 (Dipietro, 2015).

¹⁰ McShane, Nair, Rustambekov, 2011; Hoyt, Liebenberg, 2011.

¹¹ C.O.S.O. is an entity born in 1985. Its original goal was to study fraud deterrence in financial reports, but subsequently it enlarged its task to internal controls and to risk management. The C.O.S.O. still today provides companies with guidelines in these three fields. Its name derives from the first chairman, James C. Treadway, Jr. From the C.O.S.O. website, www.coso.org.

Figure 2.3 shows the E.R.M. model created by C.O.S.O. in 2004. At the top of the cube we can see the four macro objectives of a company: Strategic, Operations, Reporting and Compliance. In the side face are present the four company levels the framework should be performed: Entity-level, Division, Business unit and Subsidiary. And in the front face, the eight components to be followed in order from the top to the bottom, for every corporate objective and for every level of deepness. Those are worth to be deeply analyzed to understand the completeness and the strengths of this model.

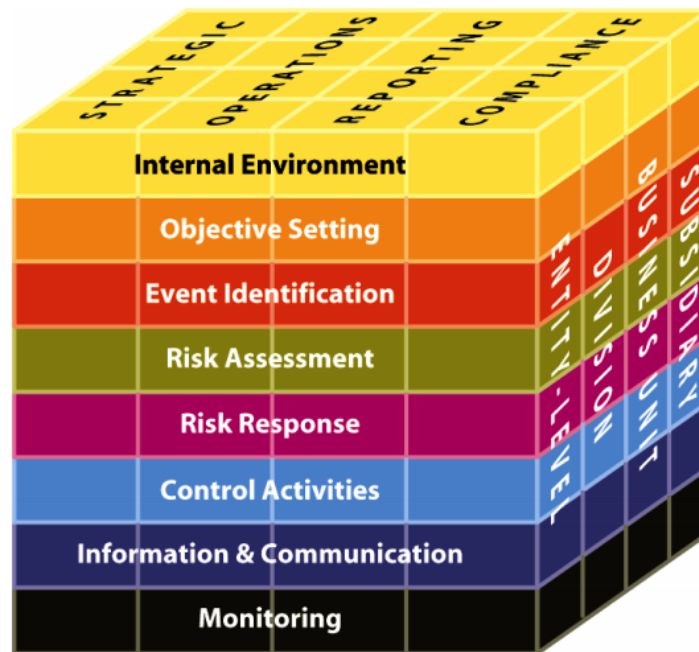


Figure 2.3: the E.R.M. C.O.S.O. framework, C.O.S.O., 2004.

Internal environment

The first component of the risk management framework is the internal environment, that must provide solid basis for all the following stages. It is composed by the entity's culture and history, the commitment to maintain integrity, to respect the ethical values set by the board of directors or by the founder and behavioral standard for the personnel. The internal environment can be further reassumed as corporate values and beliefs. The environment has to be the basement for every level of the company and everyone should be aware of it. A good vehicle to spread those information is a document called code of ethics, issued by the board of directors and listing all the principles above mentioned. The publication of the code of ethics is also one of the most important practices to adopt in order to fulfil the requirements of the legislative decree 231 of 2001.

In this phase, the hierarchy and authority are formalized and responsibilities are distributed among managers.

Internal environment also comprehends the policies (or philosophies) adopted by the company to manage risks.

One of the most important aspect to be individuated is the overall risk appetite, described by the C.O.S.O. as “the amount of risk ... an entity is willing to accept in pursuit of value” (C.O.S.O., 2004, p 28). Risk appetite is strongly tied to the corporate strategy. It provides a criterion with which to choose among different strategies to achieve the desired outcome. Strategies within the risk appetite limit shall be considered, whether strategies with a risk profile outside of it should be rejected.

Risk appetite is influenced by the company risk tolerance. The C.O.S.O. defines risk tolerances as “the acceptable levels of variation relative to the achievement of objectives, ...measured... in the same units as the related objectives” (C.O.S.O., 2004, p. 40). To summarize: risk tolerance translates the amount of risk accepted with the risk appetite in an area around the expected outcome and convert risk into units of outcome.

Risk appetite and risk tolerance should be chosen and calculated using both quantitative and qualitative methods. C.O.S.O. does not suggest how to calculate them, leaving the decision to managers. This approach provides flexibility, but may lead to overconfident managers that want to transform risk in opportunities to ride in every case, using only their judgement not supported by data. Power (2009) hypothesizes that “an impoverished conception of ‘risk appetite’ is part of the ‘intellectual failure’ at the heart of the financial crisis” (Power, 2009, p. 849), and that regulators should address the problem of managers conceiving risk too lightly. By studying some details about the mortgage crisis of 2007, it is shocking to learn how much banks, institutions and credit rating companies were underestimating the scale of what could have happened.

A solid control environment also helps to prevent fraudulent behaviors that could occur. In details, to commit a fraud the A.I.C.P.A.¹² (2002, p. 1722) suggests that there must be three elements at the same time, the so-called fraud triangle:

- Management or employees are under pressure, or have an incentive to commit a fraud. Especially if the work of the management is valuated on short-run financial indicators, there is the possibility to have questionable accounting entries;
- The opportunity to commit a fraud. A crack in the internal controls system allows managers or employees to commit frauds;
- “Those involved are able to rationalize committing a fraudulent act. Some individuals possess an attitude, character or set of ethical values that allow them to ... intentionally commit a fraud”.

¹² American institute of certified public accountants.

A sound control environment allows the company to strongly contrast the last element, the possibility for managers or other personnel to justify themselves for the fraud committed.

Objectives setting

As described at the beginning of this chapter, risk exists only after the definition of an objective. In this phase directors and managers, starting from the mission and vision, will set clear and detailed corporate objectives. The C.O.S.O. (2004) suggests to divide objectives in the four categories of the framework: strategic, operative, reporting and compliance.

Strategic objectives are those discussed at the highest level of a company and that affect the long term-survival of the company and its ability to generate value. Those choices are crucial, since many times there is no possibility to turn back or the costs to do it will be prohibitive.

Is then necessary to set sub-objectives to enable the company to achieve the strategic objectives.

Following the E.R.M. framework, we find 3 categories of sub-objectives:

- Operational objectives, affecting the efficiency and effectiveness of the operations, and setting cost targets;
- Reporting objectives, pertaining to how the financial and non-financial information issued by the company is reliable and transparent;
- Compliance objectives, associated with the respect of the regulations imposed by the legislator.

An accurate identification of the different objectives allows the following phases to be easier. Finally, all the objectives and strategies must respect the risk tolerance and risk appetite boundaries set in the internal environment phase.

Event identification

Having defined the objectives, management have now to individuate all the events that can interfere, the red dots represented in Figure 2.1. When searching for risks and opportunities, managers and directors have to consider that threats are present both inside and outside the company.

This phase could seem trivial, and in other frameworks it is embedded in the risk assessment¹³. However, the C.O.S.O. (2004) highlighted that identifying all the possible events before considering the amount of risk associated with the single event is convenient; following this approach, managers

¹³ A framework presenting this feature is for example the Internal Control Framework, issued by C.O.S.O. in 1992. The update version highlights in principle 7 that even if event identification is within risk assessment it should be considered with due attention.

and directors are forced on a mere research and classification of events. During the risk assessment phase, irrelevant events may always be dropped from the list but only after having marked them, or their joint effect, as non-significant¹⁴ for the company.

To identify events is not simple at all. In the end, it means to forecast what could happen in the future. Both quantitative and qualitative methods (or a combination of the two) can be used.

Quantitative methods are especially difficult to use in the event identification: databases of past events occurred or potential events should be implemented, that implies a huge work because of the extreme variability to deal with.

Qualitative methods are easier and less expensive, but at the same time quite imprecise and non-objective: a simple and quite effective way to identify event is conducted by referring to the past events and by speculating if they can happen again or if they can trigger new one. However, in particularly animated and troubled environments, looking to past events could be dangerous and may lead to incorrect event identification.

Once all events have been identified, the C.O.S.O. (2004) suggests to categorize the events discovered to understand if interactions among them may be present or may trigger other events.

Given the astonishing variability that distinguish the events, each company will set a different system to categorize them. There is often no need to stick with a given model, because the experience and judgement of managers are the best tools for this activity, and it is sufficient that whom who will use the list of events will understand the criteria used.

To exemplify some categories that include the most dangerous risks for a company, below is reported a table inspired by C.O.S.O. (2004):

External Factors	Internal Factors
Economic (financial markets, unemployment, competition, credit default).	Infrastructure (availability of assets, access to capital, obsolescence).
Natural environment (emissions, disasters, raw materials).	Process (design, capacity, execution, dependency).
Political (government changes, legislation).	Personnel (skills, frauds, health & safety).

Table 2.1: examples of event identification and categorization.

Risk assessment

¹⁴ Using the appropriate term that an auditor would use, non-material.

The events listed and classified in the previous step must now be deeply analyzed, and the amount of risk has to be calculated for each one. Risk is composed of two elements, to be calculated separately:

- Likelihood, defined as “the possibility that a given event may occur” (C.O.S.O., 2004, page 123). Estimations of the probability of an event are almost never easy and this complexity may lead to unprecise approximations. Complexity grows especially in case of non-recurring events for which quantitative instruments as regressions or expected trends cannot be calculated due to the lack of historical data;
- Impact, *i.e.* the effects that the event implicates if it occurs. The impact is usually calculated mostly in economic term, but may be driven by non-economic factors as the impact on reputation and image.

Both those characteristics could be calculated in quantitative or qualitative methods, or with a combination of the two. Quantitative methods comprehend the use of data to run regressions or draw trends. Qualitative methods instead require a deep knowledge of the risk, its description in detail and the formulation of estimates on the possible impact and probability.

Risk calculation is a difficult operation, made even more complex by two main factors: timing and interaction among risks.

For what concerns the timing, risks have to be calculated following the timing of the objectives. Short-term objectives cause short-term risks, easier to calculate both for the impact and likelihood; long-term strategies, instead, entail long-term risks, that require way more effort.

Interactions among risks are also complicating the calculation, especially in the case of interrelated events that could cause a chain reactions among risks.

Management considers both likelihood and impact to prioritize all the risk individuated. A useful instrument to do this is the likelihood-impact matrix: risks with high probability to happen and massive potential impact must obviously be tackled first. The matrix is shown in figure 2.4.

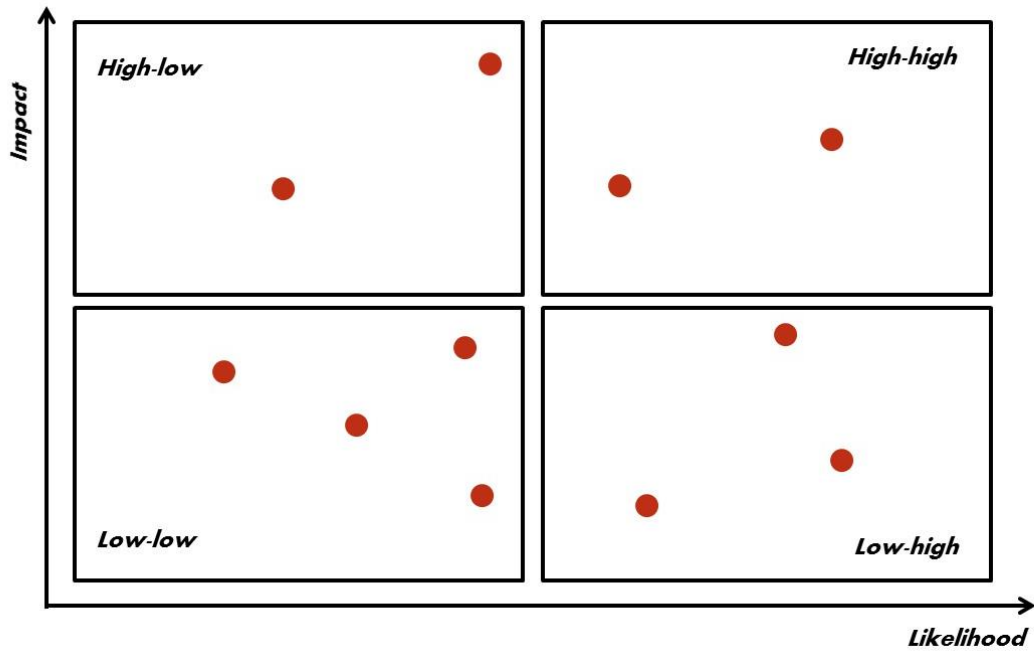


Figure 2.4: risk matrix. Author elaboration.

The risk calculated by managers is the so called inherent risk. The C.O.S.O. (2004, p 49) defines this risk as: “the risk to an entity in the absence of any actions management might take to alter either the risk’s likelihood or impact”. In brief, the total risk that the company face. In figure 2.5 inherent risk is the whole area under the distribution.

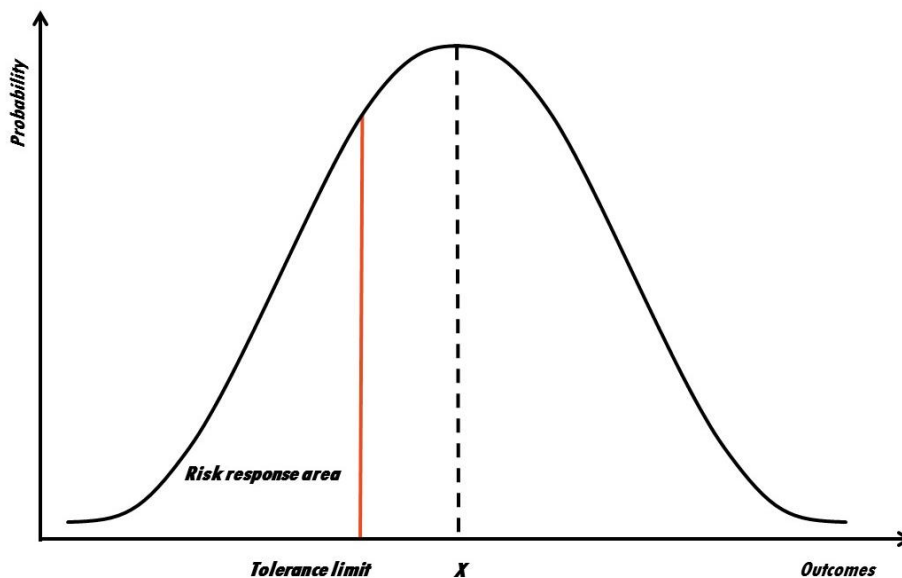


Figure 2.5: risk represented as the probability distribution around the desired outcome X. The red line indicates the tolerance limit. Author elaboration.

The risk tolerance limit set by the company in the first stage of the E.R.M. is now crucial to understand if the risk associated to an event is over the threshold and must be reduced or can be bore as is. In the

first case, reducing risk imply that management has to individuate adequate risk responses. The amount of risk remaining is called residual risk. In figure 2.5 is represented a hypothetical situation in which the amount of opportunities is the same as risks, and opportunities does not have a threshold of tolerance.

Risk response

As seen above, risk response is that phase in which risk is reduced to the tolerance limit. As suggested by the C.O.S.O. (2004), possible risk responses are:

- Avoidance: the risk is not generated by avoiding the event that can generate it, for example by exiting a market or stopping the development of a product;
- Reduction: every action taken to reduce both the likelihood or the impact. For example, by implementing a control on a process or by including in the portfolio a derivative instrument;
- Sharing: the possibility to reduce likelihood or impact by sharing or transferring a portion of the risk to a third party. A clear example of sharing risk is the practice of the syndicate loan;
- Acceptance: no action is taken to influence likelihood or impact of a risk. This is possible only if the risk is already within the risk tolerance threshold or when this barrier is considered elastic and the company choose (or is forced) to bear the risk.

In evaluating the responses, managers have to consider that costs for tackling likelihood or impact should not overcome the benefits.

For significant risks it is a good habit to figure out a range of response options, allowing the comparison of different scenarios, and most importantly to overturn the status quo and challenge the sentence “That's the way it's always been done”.

Control activities

Control activities consist of policies and procedures putting in practice risk responses identified by the management are implemented correctly and in a timely manner.

A policy represents the reason why a control is in place, and the risk it tackles; can be found written but many times is simply communicated orally to the ones performing the control activity.

A procedure is the review itself. It should not be performed mechanically but instead by focusing on uncommon outcomes or unclear explanations, and should trigger a serious investigation and alert managers.

Examples of control activities comprehend:

- Approval;
- Authorizations or double authorizations;
- Verifications;
- Reconciliations;
- Reviews of performances;
- Security of assets;
- Segregation of duties;

The above-mentioned controls can be divided in two major categories: ex ante controls and ex post controls. Ex ante controls should avoid the arising of errors and deviations from the real objective by not taking some decisions or actions. Ex post controls, instead, allow a gap analysis between the desired outcome and the reality; this is meant to correct the direction of a certain work or decision, or if a damage is already done, to find the responsible.

Control activities are not necessarily implemented as one for each risk response identified, but instead the single risk response can be implemented both by more control activities or managers can conclude that a control in place is sufficient to cover more responses identified.

Finally, it is important to clarify that controls are entity-specific. Companies with the same objectives and risks identified will almost surely tackle the control activity design differently, based on the size, the complexity of the operations and the experience of the people employed.

After massive changes in the controls system design, the residual risk should be reassessed in order to seek for risks the company is still exposed to.

Control activities are the heart of the E.R.M. model, since they are the activities that actually reduce the inherent risk to the desired amount of residual risk. A more detailed explanation is provided at in the next chapter, solely dedicated to internal controls.

Information and communication

Information is needed at every level of the company, from the top level to set the strategy to all employees for the daily operations. Effective response to risks derives from the quality of the data available.

A hard challenge for those who manage information is to translate raw data; the continuous flow both from the inside and outside of the company, from official and unofficial sources needs a solid system that can handle it.

This remodeling of data means to merge single pieces of information and let a single figure to acquire more and more meaning. An adequate information system is the instrument that allows this job. Data

management is probably one of the greatest challenges of companies today; it is extraordinarily hard to have an information system able to communicate well and with the same “language” between all its parts. For the sake of the exemplification, it could happen that the E.R.P.¹⁵, the software that collects human resources and the one used to consolidate have different data formats or coding, and different data cannot be merged easily and without manual work. A specific branch of business administration, called business intelligence, provides possible solutions to this problem.

The importance that information systems have gained inside organizations had brought also security problems: huge risks, not even considered 15 years ago, derives from malfunction or attacks to the information system or the theft of valuable data.

Information is not only used by employees and managers of a company; fundamental addressees of company information are the stakeholders, those with some kind of interest in the company. The most important information that have to reach them include company’s objectives, values and the risk threshold and tolerance.

Monitoring

The last phase of E.R.M. is reserved to the monitoring of the whole enterprise risk management system. This activity ensures the effectiveness of the model, its ability to manage risks and find the cheapest and most adequate solutions. But maybe most importantly, monitoring allows the model to match the flexibility requirements of the management. An E.R.M. system too rigid will not fit the changes that inevitably occur in a company’s lifetime, and will sooner or later be obsolete and useless. The two purposes of this phase that have been just presented are usually performed in two different ways. To check the effectiveness, ongoing monitoring activities should be planned into the design of the E.R.M., to reach the point into which the system almost “monitors itself” (C.O.S.O., 2004). Those first types of activities can be computerized or be performed by low-level managers, and should trigger a response immediately after a problem occurs. The second type of monitoring activities in place are called separate evaluations; those are *una tantum* assessment of the whole E.R.M. system, and can be carried out regularly, for example once a year, or after a substantial change has happened inside or outside the company.

Separate evaluations are one of the duties of the internal auditor. The process is executed in collaboration with the area, division or function managers, which are usually asked to self-evaluate the operations they are responsible for. Subsequently, a general evaluation of the eight E.R.M. phases is conducted by the internal auditor, that issues an opinion on whether it should be updated or changed

¹⁵ Enterprise resource planner.

in some parts, and if it is effective to catch and manage risks. Serious matters are then reported to the top management and to the directors.

The two types of monitoring activities have a clearly distinct timing and should not be confused. The frequency of the separate evaluations should depend on the risk assessment phase and on the quality of the ongoing monitoring activities. If managers or directors have some reservations about the E.R.M. system, the fast and cheap ongoing monitoring activities should be those strengthened instead of frequent separate evaluations that become redundant and are quite expensive.

It is important to highlight that the role of the internal auditor into the E.R.M. is not limited to the last component of the whole model, monitoring. Even if managers and the board of directors are the direct responsible for the risk management processes, the principle n° 2120 of the International Professional Practices Framework (I.P.P.F.)¹⁶ standards gives to the auditor an essential advisory role and the internal auditor's expertise can be used in every phase; From the creation and assessment of the internal environment to the identification and assessment of risks and the estimation on whether the information is flowing correctly and sufficiently inside and outside the company.

In conclusion, it is crucial to remember that managers of a company that provides itself with a solid and well established E.R.M. system should not feel immune from risks and should not make the mistake of over extending the risk tolerance and risk appetite thresholds. As Power (2009) states, managers of many companies before the severe financial crisis of 2007 had a "near theological belief" on the function of E.R.M. as a shield from every type and amount of risk.

E.R.M. is a powerful tool that helps to rationalize, organize and link activities as risk individuation and risk management, but the crucial barrier against risk is the prudence and the ability of managers to find effective countermeasure.

¹⁶ The document setting the international standards for the internal audit profession.

Chapter 3: Internal Controls

As seen in the previous chapter, internal controls are at the heart of the E.R.M. models, thanks to the crucial role they play into the process of reducing inherent risk to the desired amount of residual risk. This chapter will describe what a system of internal controls is, the people responsible for it and the role of the internal auditor.

3.1 Definition

There are several valid definitions for internal controls. Many of them derives from the one provided from a single source already presented above, the Committee of Sponsoring Organizations of the Treadway Commission. For this reason, this chapter begins with the definition provided by the C.O.S.O.:

“Internal Control - A process, effected by an entity’s board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations;
- Reliability of financial reporting;
- Compliance with applicable laws and regulations” (C.O.S.O., 2004, p 122).

The very first framework issued by this successful and prolific commission was the Internal Control Framework, in 1992. An update was released in 2013, and it is shown below in figure 3.1.



Figure 3.1: C.O.S.O. internal control framework, 2013 version. www.coso.org

This new framework was necessary to meet all the changes occurred in the business environment in 20 years and to absorb some features introduced by C.O.S.O. in the E.R.M. framework of 2004. The two models are becoming more and more similar, and possibly in the future the C.O.S.O. will provide a unique model for those two strictly correlated topics: risk management and internal controls.

The differences between the Internal Control Framework of 1992 and the update of 2013 have been analyzed by the audit firm Price Waterhouse Coopers in 2004, and include:

- Reporting objectives include more than just financial information;
- The suggestion that changes in the control environment should trigger an immediate response in internal controls;
- The creation of seventeen solid principles that formalize the advices present in the 1992 framework;
- The introduction of point of focus, fundamental characteristics contained in a principle;
- Consideration of third parties providing services regarding internal controls;
- Explicit consideration about the risk of fraud;
- The recognition of the importance of I.T. for internal controls.

Another very detailed definition for the internal control system comes from the Turnbull report (1999, p. 7):

“An internal control system encompasses the policies, processes, tasks, behaviours and other aspects of a company that, taken together:

- Facilitate its effective and efficient operation by enabling it to respond appropriately to significant business, operational, financial, compliance and other risks to achieving the company’s objectives. This includes the safeguarding of assets from inappropriate use or from loss and fraud, and ensuring that liabilities are identified and managed;
- Help ensure the quality of internal and external reporting. This requires the maintenance of proper records and processes that generate a flow of timely, relevant and reliable information from within and outside the organisation;
- Help ensure compliance with applicable laws and regulations, and also with internal policies with respect to the conduct of business”.

The importance of internal controls has been strengthened with the Turnbull report and, later, in the internal control guidance published in 2005 by the U.K. Financial Reporting Council¹⁷. This document states that a sound system of internal controls:

- Contributes to safeguarding company’s assets;
- Improve efficiency and effectiveness of operations;
- Enhance the reliability of reporting;
- Assists the compliance with regulations;
- Helps in the detection of frauds.

3.2 Actors involved

The Turnbull report suggests that internal controls should involve many people inside a company at all levels. The various tasks are explained below.

The board of directors, as for the provisions present in the British and Italian corporate governance codes seen in Chapter 1, is responsible for the establishment of a safe and sound internal control system. To accomplish this, the directors set policies, *id est* the overall direction, and seek for assurance about the effectiveness of the internal controls.

To achieve valuable results, internal controls cannot be perceived only as a sterile, compulsory step executed by somebody, or even as a bottleneck. If the control environment is developed enough and

¹⁷ Successor of the Treadway commission.

understood by everybody, internal controls can be seen by the individuals who have to apply them as a fundamental concept running across the whole company, in which everyone should be interested in. To achieve this, the core components are the trustworthiness of whom design the controls and their ability to communicate the importance of the system; those capabilities must belong to the management, those who run the function or division they are responsible for and who should be aware of the risks in place and know the methods to reduce them. They have to execute directors' policies by designing and implementing the internal controls, updating them periodically and checking that the controls are applied correctly.

All employees should acquire the necessary knowledge not only to use internal controls, but to "become part" of them; by understanding internal controls employees will be able to contribute to their improvement and will apply them as they have been thought and designed.

The internal auditor fits into this scheme with a supporting role. He "must assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement" (I.I.A., 2016). This definition gives to the internal auditor different roles. He provides consultancy services to managers, both through the recommendations at the end of an audit carried out or prior to the design of the system, if asked. He refers directly to the board the results of the assessment done about the operativity of the system and he is also able to provide assurance to the stakeholders that sound controls are in place to preserve the company.

All the bodies composing the corporate governance of a company interact and examine the internal control system for different reasons. Audit firms must assure that internal controls cooperate to give correct and transparent information. Performance audit must evaluate the cost effectiveness of controls. The audit committee directly overlooks the work of internal and external auditors and ensures that adequate controls exist to signal if company is in compliance with applying regulations. The relationships among the actors of the internal control system are not as straightforward as it may seem. Often, tasks and duties of the different bodies overlap and create a confusing situation.

To summarize, below is presented a table which represents the tasks of everybody in relation to the company objectives of the C.O.S.O. internal control framework represented in Table 4.1.

Actors	Operations	Reporting	Compliance
Board of Directors			
Managers			
Internal Audit			
External Audit			
Performance Audit			
Audit committee			






-  Direct control and monitoring
-  Design and implementation
-  Monitoring
-  Supervision over other actors
-  Minor activities

Table 4.1: Actors of the system of internal controls and their duties. Author elaboration.

3.3 Internal controls characteristics

Controls are in place to help achieving the objectives set by reducing the inherent risk to a predefined level of residual risk. Pickett (2010) illustrates that an effective control should be:

- Oriented to the riskier aspect of a process or operation and not on the details;
- Clearly defined and fully understood by the users;
- Realistic and not too lumbering;
- Agreed between the management and the staff performing it;
- Monitored to assess the extent to which it is being applied in comparison to the original design;
- Measurable;
- Timely.

The design of a system of internal controls is very complex. Many factors have to be taken into consideration, and still there cannot be the certainty of a sufficient the risk reduction. Turnbull (1999, p. 7), reminds that:

“A sound system of controls reduces, but cannot eliminate, the possibility of:

- Poor judgement in decision-making;
- Human errors;
- Processes being deliberately circumvented by employees and others;
- Overriding controls;
- The occurrence of unforeseeable circumstances.

A sound system of internal controls therefore provides reasonable, but not absolute, assurance that a company will not be hindered in achieving its business objectives”.

Similarly, the C.O.S.O. warns in the internal control framework of 2013 not to be over confident towards the infallibility of an internal control system.

Pickett (2010, p. 289), defines this problem as “the fallacy of perfection”. Adding more and more controls to a process or activity ensures risk reduction, but is also costly in terms of money and time spent in controlling. Procedures and rules cannot ensure success.

A new type of controls has gained importance in the last few years, called soft controls. They should not be considered a replacement of manuals and procedures, the so called hard controls, but instead as a complement to it. Soft controls are meant to provide an understanding of how much managers and the people who have to apply the controls feels embedded in the control environment and aware of their role they have in it.

To reassume, having less controls performed with a grain of salt and well monitored by the competent actors is better than having a cumbersome and complex system of internal control that is not understood by the majority of the people of a company.

Chapter 4: Internal auditing

After having discussed about the three different “levels of deepness” the internal auditor is involved in a company and its role inside the organogram, this chapter will now define what internal audit means and to which tasks it is associated.

Firstly, we will introduce the path throughout internal audit gained importance in the business world, making a comparison between the U.S. and the Italian case. This comparison adds value to the research because as we have already seen in the previous chapters, the Italian case evolved by learning mainly from the Anglo-Saxon world.

Then, we will discover the definition and the professional framework of internal audit issued by the international professional association.

Successively, we will focus on the main objectives of internal audit, through the professional Standards.

Finally, the most conspicuous part will be dedicated to the main internal audit approaches and the “field work” conducted on a daily basis.

4.1 Audit history and today’s spread of the function

The term auditing comes from the Latin *audire*, that means “to hear”. The etymology derives from the fact that auditors have to evaluate processes or activities in which he is not usually involved, and before starting his or her activity, listening and acquiring information is fundamental for the success of the job.

Auditing is an ancient practice, almost as old as accounting: it evolved principally from the assurance need expressed by various stakeholders, incapables of gathering the information needed about an organization. Auditing, including in this term both the internal and external universes, serve the society by monitoring performances and enforce accountability of managers and of those charged with governance. Internal auditing evolved as a branch of external auditing. It is not easy to identify an agreed dawn for this profession. The only guaranteed starting point is the foundation date of the Institute of Internal Auditors (I.I.A.), occurred in the U.S. in 1941 by a group of only 24 internal auditors. Internal auditing was then widely perceived by managers and employees as a continuation of the external auditor’s work, and the job extension was limited to accounting-related functions, with no or limited influence in managerial decisions (Ramamoorti, 2003).

Only after World War II the U.S. scenario saw an enlargement of internal audit tasks: no more only accounting related matters, but the involvement in different types of operations with the goal of enhancing the total profitability of an organization.

By 1957, internal auditors were required by the I.I.A. to provide five major services:

- Reviewing internal controls;
- Reviewing compliance with the regulations;
- Reviewing the reliability of accounting documents;
- Reviewing the quality of performances;
- Safeguard assets from misappropriation, losses and misstatements. (Ramamoorti, 2003).

At the same time, the Institute was growing and aiming to obtaining more and more recognition as a separate profession, through the spread of the internal audit Standards. The profession spread following the pace of the increasing attention to controls inside companies, both inspired from the will and foresight of managers and directors and obligated by the legislators.

In 1977, the Foreign Corrupt Practices Act in U.S. empowered the internal auditors in their role of the implementation and improvement of internal controls over accounting processes (Adams, 1994). By the early 1990s, and the necessary mention of the publication of the C.O.S.O. report in 1992, internal auditing evolved an approach for the review of internal controls strongly based on risk assessment. The profession kept growing, thanks to the increasing awareness of managers and directors of the benefits associated with an internal auditing. Spikes of that awareness emerged in the early 2000s, during the period of financial scandals as Dotcom and Enron. Moreover, law requirements accelerated the propagation of internal audit in U.S. companies. The Sarbanes-Oxley Act of 2002, in Sections 302 and 404, required managers to develop and monitor a system of internal controls over financial reporting and to disclose those controls and related procedures; both requirements in which the internal auditors could have a critical role. In fact, the I.I.A. wrote in 2004: “Internal auditors are frequently pressured to be extensively involved in the full compendium of Sarbanes-Oxley project efforts as the work is within the natural domain of expertise of internal auditing” (The I.I.A., 2004, p. 10). Finally, in 2003 the NYSE passed Section 303A, requiring the presence of an internal audit function in every listed company (Protiviti, 2014).

For what concerns the history of Internal auditing in Italy, Tettamanzi, in 2000, described internal auditing in Italy as a new phenomenon, growing and at the time present mostly in medium-big companies. Another study conducted by the Italian internal audit Association¹⁸ in 2006 revealed that

¹⁸ A.I.A.: Associazione Italiana Internal Audit.

within a sample of more than 350 Italian companies, only one third had an internal audit function established before 1995 (Lo Dico, 2008).

The function spread in Italy with a major contribution coming from the legislator. As we saw in Chapter 1, the first intervention for internal auditing was in 1998 with the consolidated law on finance, then in 1999 the Preda code, in 2001 the legislative decree 231 and finally in 2005 the law 262 called law on savings. Especially the Italian corporate governance code opened the way for the presence of an internal audit function in every listed company. As reminded in Chapter 1, the code was born with pronounced flexible features. Therefore, its provisions are strongly recommended for listed companies, but not mandatory, following the comply or explain principle.

Nowadays, as from a study of P.W.C. dated 2016 reports, only 6% of Italian listed companies disclosed to have made the choice of not establishing an internal audit function (2% did not disclose this information). The main reasons of this choice are linked principally to two reasons:

- Limited dimensions of the company;
- The structure of the group; Some groups set an internal audit function at single company's level, therefore the holding decided not to implement it.

4.2 Definition

The best definition of internal auditing has been found in the website of the I.I.A.:

“Internal auditing is 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”.¹⁹

From this definition, it is necessary to isolate and analyze some key concepts.

Internal auditing must be independent and objective. This is the reason why internal audit function must report directly to the board of directors and has unrestricted access to senior management and to the board itself, along with unrestricted access to all the information needed to accomplish its objectives. The independency is evaluated yearly and any threat to it must be communicated as soon as possible to the board of directors.

Internal auditing is an assurance and consulting activity. The assurance function derives from the roots in common with the external audit. Instead, consultancy means that internal auditors may

¹⁹ www.na.theI.I.A.org , the website of the Institute of Internal Auditors, North America.

provide advices to managers to accomplish the company objectives in an efficient way. Those activities must create value for the organization. Even if it is a very difficult task to accomplish, a system to evaluate internal auditors' performances should be in place.

Internal auditing is characterized by a systematic and disciplined approach, with professional standards and rules to use as a guideline. All the actions made by the auditors should be planned.

The overall scope of the C.A.E. is to evaluate and improve the effectiveness inside an organization, and to be an appraisal service for the organization as a whole. In fact, the internal auditor performs in all the corporate levels before explored: corporate governance, risk management and internal controls.

The I.I.A. does not only provide the definition of internal auditing. It published in October 2016 the last update of the International Professional Practice Framework (I.P.P.F.), a document modified several times through the years that contains the mission, the definition, the code of ethics, and the professional standards.

To better define what internal audit is, it is useful to read the mission declared in the I.P.P.F.:

“To enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight”²⁰.

The I.I.A. also provides the internal auditors with a code of ethics, behavioral principles to follow while performing an audit or approaching any issue:

- Integrity: the internal auditor must demonstrate honesty, diligence and responsibility, follow regulations;
- Objectivity: not to be influenced by its own interests or by others in forming judgements;
- Confidentiality: respect the value and ownership of information and do not disclose without authority;
- Competency: apply knowledge, skills, experience and constantly improve its effectiveness of service and apply the standards.

The code of ethics seen above lists characteristics very similar to those applicable to the external auditors; in fact, the final purpose of providing assurance to the stakeholders is shared between the two professions.

The main component of the I.P.P.F. is the set of standards for the profession. The standards are a set of principles that provides guidelines to the internal auditors about how to perform their work.

²⁰ www.na.theiia.org

In the introduction, it is explained the overall scope of the standards, that is to:

- “Guide adherence with the mandatory elements of the International Professional Practices Framework.
- Provide a framework for performing and promoting a broad range of value-added internal auditing services.
- Establish the basis for the evaluation of internal audit performance.
- Foster improved organizational processes and operations”. (The institute of internal audit, 2016 p 1).

The I.P.P.F. Standards are divided in two main parts. The first part lists the Attribute Standards, that affect the connotations that the organizations or the people involved in internal audit activities must or should follow. The second part sets the Performance Standards, that describes the nature and the activities of internal auditing.

The standards are very broad and leave to the internal auditors quite some free space in its boundaries, as we would expect from a set of principles that must be interpreted according to the situation and the resources the internal auditor encounters in conducting his or her work. The next paragraph will try to explore the different interpretations of the standards.

4.3 What standards requires a C.A.E. to do

Pickett (2010), affirms that among the big majority of the definitions of internal auditing there are similarities. The main points in common are the independence of the internal auditor and the reviewing of the organization internal control system. Apart from those fundamental key concepts, “there is no right model of internal audit and the final role adopted depends on [those] elements:

- Attitudes and views of the [internal auditor];
- Best professional practice;
- Expectation of the organization;
- Skills and capabilities of the audit staff” (Pickett, 2010, p 318).

The least logical point could appear the one about the expectations of the organization, that might clash against the idea of an independent and objective auditor. Internal auditors cannot do what managers want them to do, because this will be a downgrading to simple consultants. Instead, this point wants to indicate that internal auditors must aim for the achievement of the company objectives.

The mix of those four elements will automatically define the model of internal audit that will be applied in an organization. Therefore, a wide range of different types of internal audit styles may exist, both for the characteristics chosen by the chief internal auditor and for the perception that people inside the company have of the internal audit function. Only if trustworthy and reliable the internal auditor will be able to provide consultancy and advise to managers.

For the sake of the explanation, some examples follow. Arena, Arnaboldi and Azzone (2006) analyzed the internal audit functions in six different Italian companies and found out a number of different shades in internal auditing; in their study, some internal audit functions were only focusing on compliance to rules and procedures, and were seen as “watchdogs” (page 286), some other hired staff personnel from other company functions and the maximum time inside the function was 3 years, in order to maintain the contact with the operations, in other instead internal auditors had a strong background in accounting or auditing, and provided quality consultancy services. Pickett (2010, p. 386) describes a common scenario in which especially more experienced managers could see internal auditors as a “hit squad”, people which find pleasure in signaling the errors of their colleagues. This situation by the way is not a wrong or strange expectation, but instead a legacy of the past, in which surprise audit were often performed as a standard way to find problems. This conduct is no longer acceptable from an auditor, that should instead evaluate together with managers or the employees of a certain function or division the best way to solve a problem. The standard way to conduct an audit will be described further on in this chapter.

The mix of the elements seen above and the expectations and prejudices may make it harder to establish clearly what internal audit function is and what does in a company. “Managers often ask auditors exactly what are they responsible for and a variety of responses may be received” (Pickett, p. 313). Attribute Standard 1000 solve this issue by requiring to the chief internal auditor to establish and review periodically the audit charter, the model of internal auditing that fits the company. The audit charter is a document that set the “purpose, authority and responsibility of the internal audit activity” in that specific company (The institute of internal auditors, 2016, p. 2).

The audit charter is approved by the board of directors, includes the main components of the I.P.P.F. and the nature of the assurance and consultancy services provided by the internal audit function.

The scope of the internal audit charted is to allow both the internal audit staff, all the people inside the company and all the stakeholders to understand clearly what internal auditors are expected to do in a specific company and which are their boundaries. It is an easy way to fight the roots of prejudices and misconceptions about what internal audit is.

Performance standards set the scope of internal auditing at the three levels of deepness: corporate governance, risk management and internal controls.

Standard 2110 requires the auditor to provide consultancy to the directors for what concerns:

- “Strategic and operational decisions;
- Overseeing risk management and control;
- Promoting appropriate ethics and values within the organization;
- Ensuring effective organizational performance management and accountability;
- Communicating risk and control information to appropriate areas of the organization;
- Coordinating the activities of, and communicating information among, the board, external and internal auditors, other assurance providers, and management”.

As we can see, these objectives are very similar to the four set by the C.O.S.O. E.R.M. framework: strategic, operation, reporting and compliance. In fact, the I.P.P.F. Performance Standards can be seen as the path the Internal auditors have to follow to reach the macro objectives included in the C.O.S.O. In two different Standards, 2120.A1 and 2130.A1, the I.I.A. lists those which for Pickett (2010, p319) are the main elements of the scope of internal auditors:

- Achievement of the organization’s strategic objectives. It is the reason to invest resources on every corporate function, the return got from an investment, and the definition of effectiveness of a function;
- Reliability and integrity of financial and operational information. Internal auditors review the means to get financial and informational information and the results of this process. The assurance goal of internal audit passes through here;
- Effectiveness and efficiency of operations and programs. Internal auditors appraise whether the processes are conducted as they were planned and are well aimed at the corporate objectives and if resources could be employed in a better way;
- Safeguarding of assets. The assurance provided by internal auditors translates also in the maintenance of the value and investment of the shareholders, and prevent or find asset misappropriation or misstatements;
- Compliance with laws, regulations, policies, procedures, and contracts.

Those five elements must be always taken in consideration as the wide scope of internal audit for what concerns risk management and internal controls review.

4.4 Audit approaches

The first choice that the C.A.E. must do is between transactional audits and system audit. This resembles more to adhere to a philosophy rather than selecting an operational way to conduct an audit.

Transactional audit

The transactional method suggests to focus on process or the operation audited and not to consider the context in which it is embedded. This allows the auditor to be very precise, but miss the interdependencies that are present among a company. This approach recalls immediately the Traditional Risk Management (T.R.M.) framework seen in Chapter 2, and its silos analogy. Transactional audit cannot be considered optimal because of the obvious limitations it has and it is generally considered obsolete, but for simple and limited internal audit function it could be used. This does not mean that solid internal audit functions should not use it at all. Transactional audit can be used for those occasions in which other bodies of the internal control system require an assessment of a specific issue or function or where a specific problem is investigated by the auditor.

System-based audit

System-based audit is the most common approach. A system is defined by Pickett (2010) as a series of resources organized in processes to reach the corporate objectives, with controls in place to secure the wanted outcome. Systems could be designed in every dimension and shape, and the fundamental characteristic is that interrelations are present among them. By conducting a system-based audit, the internal auditor cannot focus solely on resources, processes, controls, or verify whether an objective has been reached. Instead, the system has to be verified as a whole, considering all the cause-effect relationships among those four elements. From here, the term “system” will be used to represent business unit or function, using the same notation of Pickett (2010).

After the adhesion to a “philosophy”, if the C.A.E. has chosen the system-based audit he has now to select the preferred of those two major approaches:

- Risk-based;
- Control Risk Self-Assessment (C.R.S.A.).

It is important to point immediately that the C.R.S.A. approach is an evolution of the first one. The popularity of the risk-bases approaches derives from the opinion that they are “a valid interpretation of the assurance role of internal auditing” (Pickett, 2010), and at the basis of modern way to conduct

internal audit. This conclusion derives from the fact that an audit guided by risks is more able to be effective and efficient than an audit steered from other drivers. Risks provide a strong guidance both to prioritize the work and to understand the nature, timing and extent of the audit to provide reasonable assurance to the C.A.E.

Below are presented the main characteristics of the two approaches. Both have in common the specific steps of an audit process, that will be presented in detail later in this chapter.

Risk-based approach

The risk based approach embrace the E.R.M. conception of controls as a way to mitigate risks. Controls are not the center of this approach, but rather an instrument to pass from inherent risk to a manageable amount of residual risk.

Following some of the basic points of one of the most used E.R.M. frameworks, the one published by C.O.S.O. in 2004, the internal auditor should follow those steps:

- Identify clearly the strategic objectives that the process we are auditing aims to reach and the company-wide objectives that the process could affect.
- Identification and detailed description of the risks. In this phase, it is very important to involve managers. They have most probably more knowledge and expertise about the process than the internal auditor, and they probably are aware of the risks present. There are three main methods to help managers in the identification of the risks:
 - Top-down. Managers are guided by instruments (as questionnaires) created at corporate level.
 - Bottom-up. Managers are left free to recognize risks, without interfering.
 - Top-down, bottom-up. Corporate strategic objectives are expressed as process sub-objectives, and only after the manager have the possibility to identify risks.
- Risk assessment, estimating likelihood and impact. Also in this phase the contribution of managers will facilitate the work of internal auditors.
- Valuation of the design of the controls, and only after ascertaining the effectiveness of them.
- Communication of the opinion and advice managers. The communication will cover the whole system audited, not only the single issues identified.

The risk based approach requires a high level of expertise and knowledge of the business form the internal auditors, that have to face specific operational objectives and risks.

Control risk self-assessment

As said above, C.R.S.A. is an evolution of risk-based approach. C.R.S.A. introduces a stricter collaboration between internal auditors and process owners in the risk management and control of an organization; managers are required to self-assess their system or process, following the first 4 steps saw for the risk-based approach. The fifth step will be substituted with actions to improve issues or weak spots revealed by the valuation process.

Therefore, if in the risk-based approach internal auditors were stepping over the borders of manager's system to individuate objectives and risks, in this approach managers play the part of the auditors in the evaluation of controls and processes.

This approach could be implemented in a variety of ways, depending on the role of the internal audit function. A more a gradual approach would see the internal auditors sponsoring this initiative, supporting managers in all the phases, carry out the work in mixed teams, making a lot of training sessions.

A harder approach, would see a lighter involvement of the internal auditor, with much more advise, and consultancy services provided and less field work.

The potential benefits of this model include more awareness of the management of its role in the internal control system, the empowerment of all the personnel working in the system and, above all, much more effective corrective actions. This latter effect derives from the fact that too often managers see as imposed the advises given by the internal auditors about how to improve a process or how to change a control. by going through the evaluation process, managers are more willing to put into practice the corrective actions self-individuated.

C.R.S.A. is for sure not an easy approach to introduce into a company. It requires a solid and reliable internal environment and a widely-shared code of ethics, the willing of the managers to bear additional work and to receive education and training in audit techniques.

Without those elements, it would be impossible for the top management, the directors and the C.A.E. to trust the results of a self-assessment made by those responsible for a system or a process. If one or more of those elements are lacking, it is better not to consider the implementation of this approach or the costs could be greater than the benefits.

4.5 Audit field work

Until now this chapter presented what internal audit is, what the Standards published by the I.I.A. requires the C.A.E. to take care of and which are the roles and approaches he can choose among to perform its assurance and consulting tasks.

This paragraph will present the various stages for performing an audit, basing on the risk-based approach, more common than the C.R.S.A. This theoretical subject has been left for last because it is strongly linked with the empirical part of this thesis, starting from the next chapter, in which we will try to study what internal auditors actually do and which instruments and techniques they use while performing field work. Thus, it is necessary to present which are the theoretical best practices in internal audit to have a benchmark with which compare the results of the empirical study.

Already in 1978, *“the basic steps in an operational audit had been sequenced as follows: perform a preliminary survey; develop the audit program; perform the fieldwork; prepare the working papers; develop a list of, and prioritize, audit findings; discuss findings with the auditee; and, finally, prepare and present the audit report”* (Ramamoorti, 2003). The basis is the same even forty years later. The most interesting and operative step, that characterizes the audit profession, is the field work, that for this reason gives the name to this paragraph and will be analyzed more in deepness.

The steps we will present cover a greater time span than those seen above, and are:

- Annual audit planning;
- Preliminary survey;
- Engagement programme and engagement planning;
- Field work;
- Reporting;
- Follow-up.

Annual audit planning

Planning is fundamental to achieve the best results possible with the annual budget resources the C.A.E. has to conduct all his or her tasks. *“It is impossible to audit everything. Auditors must be seen to be doing important work”* (Pickett, 2010, p 789). With experience and solid preparation, the C.A.E. is able to detect which are the most important areas that should receive and audit, and the level of difficulty they entail. The planning phase is very important for the distribution of the resources available for the internal audit function. Senior auditors should obviously face more serious, high-risk issues, whether junior auditors should tackle more routinely work.

In this phase, the C.A.E. must consider several variables. Among the most important: organizational objectives, audit charter, management’s needs, budget for the function, personnel available.

With those in mind, the C.A.E. sets the plan following the steps shown in Figure 4.1.



Figure 4.1: Audit plan steps. Liberally inspired by Pickett (2010), p789.

The solid base for a plan are naturally the objectives to reach. Company objectives must be clearly defined by the top management and the board of directors and communicated to the C.A.E. when he is not involved in this phase.

The next step requires the individuation and assessment of the major risks of a company. Risks individuated are usually labelled for typology (operational risk, credit risk, strategic risk, market risk, etc.), as seen in Chapter 2.

Risks then must be assessed, valuating likelihood and impact. This phase is fundamental to prioritize them and decide nature, timing and extent of the audit work to conduct. For the prioritization of the risks a useful tool is the risk matrix, already shown in Figure 2.4. The C.A.E. must set the entity-level materiality to decide which risks should be considered and which not.

After having prioritized risks, the C.A.E. can start building the audit strategic plan. It reconciles the workload just quantified with the resources, both in terms of budget and of human capital, the audit function is in possess. The audit strategic plan draws the path that the audit function has to travel to reach the C.A.E.'s objectives for the year, and accounting for the budget.

Finally, a formal audit plan is released, resuming all the previous steps. The audit plan normally covers cyclically the areas with the greatest impact over the main corporate objectives. This provides general assurance about the adequacy of internal controls.

The audit plan must be approved by the bodies from which the audit function depends: the board of directors in Italy and the audit committee for the Anglo-Saxon countries.

Quarterly plans are usually derived from the annual plan. This is useful especially in turbulent, fast changing contexts, in which risks could vary a lot over time; quarterly plans can be adjusted without affecting the others.

The single audits are then assigned to the people composing the internal audit staff and the process owners are advised of the incoming audit²¹.

Preliminary survey

This is the phase where the internal auditor accumulates all relevant information over the system or process he has been assigned by the C.A.E.

Keeping in mind the fundamental objectives set by Standard 2120.A1 (reliability and integrity of information, compliance, safeguarding assets, efficiency and effectiveness) the internal auditor meets the process owner and tour the operational area. A strong collaboration with the manager allow the internal auditor to gather more information. Objectives, scope and timing of the audit will be agreed with the manager (Pickett, 2010).

A simple checklist of information to gather is:

- Operational objectives;
- Structure and organization;
- Most important processes;
- Regulation and internal rules;
- Human resources;
- I.T. system;
- Significant risks;
- Current measures to manage risks, key controls.

This phase could be eased by analyzing past internal or external reports and work papers. If key risks and procedures have been already individuated recently, a lot of time can be saved by just verifying the correctness of the information available. Preliminary survey, as every other step of an audit that requires to work in contact with the people of the audited system, should create the least possible discomfort.

The internal auditor could use several techniques: surveys, corporate documents, flowcharts, and direct observation (Lo Dico, 2006).

Since the preliminary survey sets the foundation of the whole audit, it is common practice to appoint a senior internal auditor to conduct it, and let the juniors do the next step, the field work.

²¹ Audit specifically set to investigate over frauds will not generate notification to process owners for obvious reasons.

Engagement programme and engagement planning

After the preliminary survey, the Standard 2240 requires the creation of the engagement programme (or audit programme). The Institute of Internal Auditors (2016) defines it as “A document that lists the procedures to be followed during an engagement, designed to achieve the engagement plan”.

The audit programme will be simpler for compliance and probity²² audits, where fewer elements are taken into consideration. Instead, for the audit of a whole system, there should be much more work into the identification of the perimeter to be audited. The more the system to be audited is complex, the clearer the definition of it must be.

Audit programme should usually contain:

- The various tasks (the nature) to be performed by the audit staff;
- The extent of work;
- The timing of tasks, with target dates.

The audit programme should be used more as a guide by the personnel that will conduct the audit, not as a holy text. A variable degree of freedom should be left to the staff to select additional or different tools to form an opinion.

The programme is an internal document used only by the internal audit function, and should be formalized into the engagement (or assignment) planning. Performance Standard 2200 defines it as a document that sets the objectives, scope, timing and the allocation of resources.

It should include:

- The terms of reference issued by the C.A.E. or senior internal auditors;
- Scope of work: a general definition of what is the audit staff there for;
- Key stages and target dates;
- The audit staff employed, with an indication of both internal resources and external advisors;
- The areas in which the components of the audit staff are assigned;
- A definition of the boundaries of the system audited;
- Main risk areas;
- Definition of the reporting methods;

It is now time for the internal auditors to put in practice the audit techniques.

²² The controls over the adherence with the code of ethics.

Field work

The audit staff in charge of the execution of the audit, equipped with the solid guidance of the engagement programme and planning, must first of all acquire direct knowledge about the audited system. Information gathering is not only necessary to deeply understand what the “field” is, but also to verify if the superficial data acquired in the preliminary survey are correct and to get an idea of the operations and to capture the flow of documentation and information.

This very first phase is carried out mainly by interviewing managers and operational personnel, observing the normal work done in an area or by carrying out walkthroughs. This latter test is performed by an auditor by slowly following a process, a job or the path of a document or piece of information from the beginning to the end.

Mapping the system

With this confidence acquired, the audit staff proceeds by mapping the processes and the controls in place. It is one of the most useful tool at the beginning of an audit to ascertain the system and define the boundaries of a system.

One of the easiest methods available to map processes is by describing it narratively. By the way, it is an available option only for very simple and narrow tasks.

Much more used are flowcharts.

Simple flowcharts, or block diagrams flowchart, is easy to create and to understand by everyone. It simply describes processes or controls in same-shape boxes.

A slightly more advanced technique is detailed flowcharting, in which boxes are designed in conventional²³ shapes according to what they represent. It is more intuitive but auditors have to be trained to understand and use it.

An example of detailed flowcharting is shown in figure 4.2.

²³ One example is represented by the Rutteman convention.

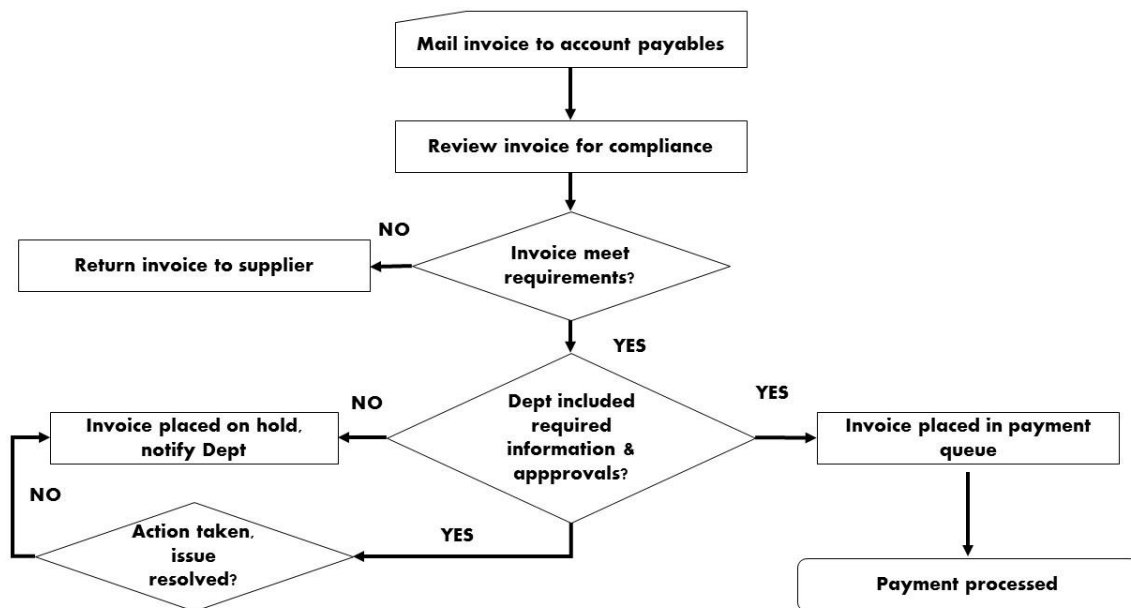


Figure 4.2: example of detailed flowcharting. Author elaboration.

Flowcharting is a powerful instrument that displays: the personnel and its role, the main documents or pieces of information, key risks and the controls required on them. In evaluating key risks, internal auditors have to establish the level of materiality. To do this, the most used tools are using predetermined ratios to apply to economic figures as annual revenues, equity or similar.

Evaluation

With the situation completely mapped out and with the suggestions from the engagement plan, the audit staff is now able to individuate and assess key risks, evaluate if controls are adequate and conceive a first evaluation.

For Pickett (2010, p. 864), this stage “provides an opportunity for auditors to apply professional creativity to the fullest”, in order to understand if controls in place are:

- Well designed;
- Effective;
- Applied as the design suggests;
- Efficient.

Flowchart is for sure a solid starting point because the results obtained draws the real situation, that is immediately comparable with the theoretical scheme that should be in place from corporate

manuals. If evidences of discrepancies with the theoretical scheme arise, the auditors should perform compliance test do better inspect the reasons and the possible implication of this issue.

Further investigations are necessary even if flowcharts do not highlight any problem with the controls. The most common are:

- Tests on specific suspicious or critical transactions;
- Surveys and inquiries on personnel or third parties;
- Reperformance of some transactions;
- Observation of the personnel performing a control;
- Inspect physical goods or documents.

Those tests could be used also in the testing phase, so they will be deeply explained in the next paragraph together with the other test typologies.

There are almost no limits to the nature of tests performed and their extent. During the evaluation of processes and controls, key factors are the internal auditors' expertise and judgement, that will allow him to form the first opinion as the audit goes on.

This control testing phase is indispensable for the formation of the first audit opinion. In fact, in the metaphor of the evidence bucket shown in figure 4.3, tests on controls represents the bottom of bucket. The auditor should gather enough evidence to support his or her findings and the first opinion conceived. The evidence bucket is no more filled when the internal auditor reaches a reasonable level of assurance²⁴.

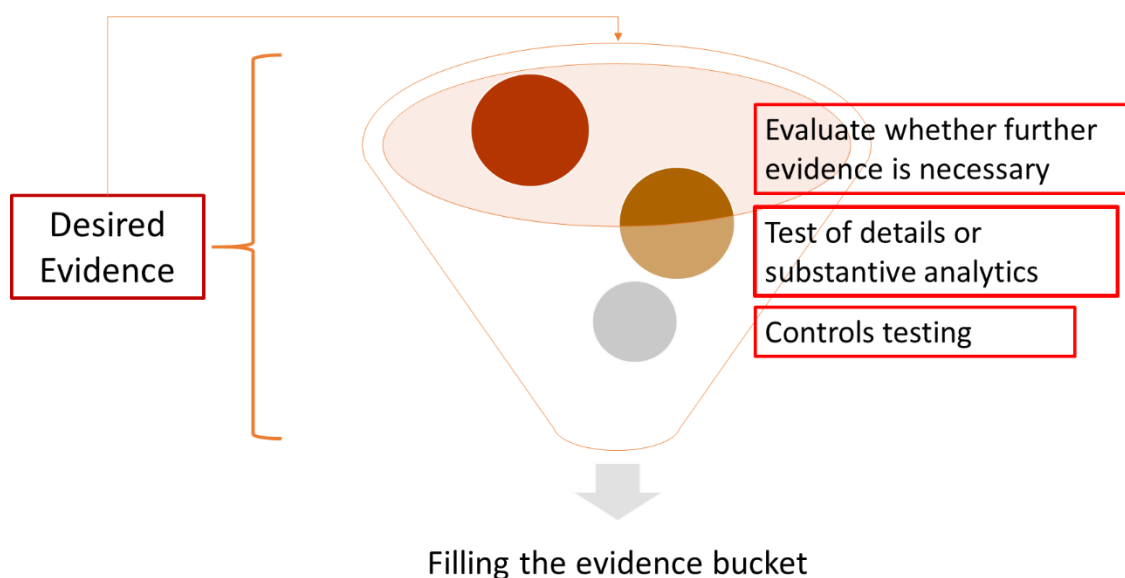


Figure 4.3, the evidence bucket. Liberally inspired from Eilifsen et al. (2010).

²⁴ Reasonable means “a high level of assurance”, IAASB (2015).

The adequacy of a controls, as mentioned before, do not only means the testing of its design, but also if the personnel performs it in compliance with the way it is designed.

After the tests on controls, the audits staff applies the protocol shown in figure 4.4.

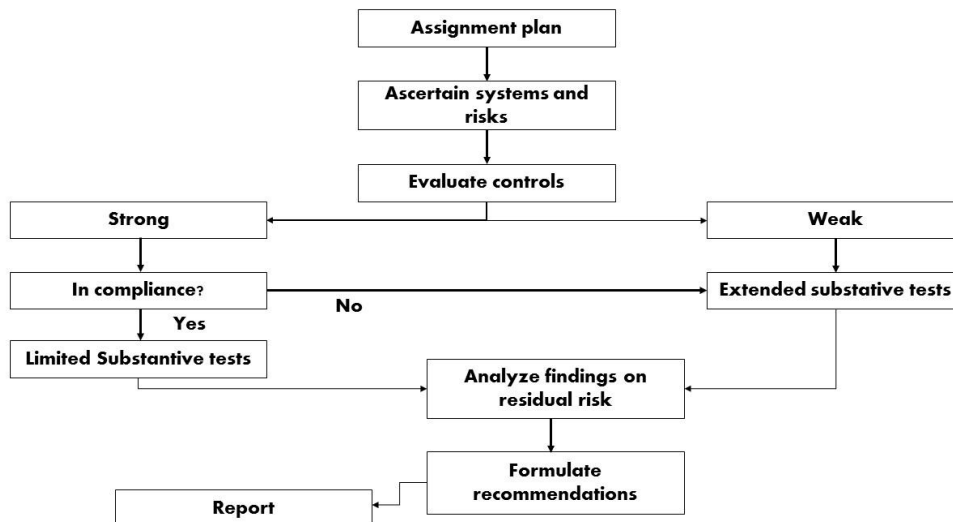


Figure 4.4: Evaluation of internal controls protocol. Pickett, 2010, page 513 and 880.

Testing

Tests on controls highlight the weaknesses of the internal control system. The weaker the control, the longer and deeper will be the substantive tests and the fuller the “evidence bucket” will become. However, it is impossible to test each control, thus the internal auditor may use the risk matrix shown above to prioritize the most important controls to focus on.

To understand if the audit staff has to perform limited or extended substantive tests on a control it is not sufficient to look only at the control. Another fundamental variable is considered: materiality. If the control is considered strong but the impact of the risks on the process is material, the judgement of the internal auditor may suggest to perform extended substantive tests as well.

The internal auditor is free to decide which test to use to conduct the audit. The decision depends on several factors (Pickett, 2010):

- The type of risk individuated: controls are inadequate compliance issues lead to different tests on te controls;
- Management concerns about the system of internal controls;
- Previous audit cover;
- Internal auditor’s experience;

- Managerial inclination to support the audit;
- Audit objective;
- Materiality of the item reviewed;
- Time available.

Also the nature of a test affects considerably the level of assurance obtained: tests conducted personally will be more reliable than indirect tests, in which the internal auditor has to trust the manager or the employees.

We will now list the manual tests that an internal auditor could perform and their main properties:

- Inquiry: questions to managers and employees about the controls, via surveys or interviews;
- Observations: asking to managers or employees to show how they conduct a control;
- Physical Inspection: counting or checking documents, goods, raw materials etc.
- Reperformance: going through a process or a control personally;
- Walkthrough: as mentioned above, it means following a good, a document or a piece of information from the beginning to the end of a process, in order to see which controls are in place, who does what and in how much time;
- Reconciliation: checking if the figures seen in a document or a database correspond to those gathered from another source;
- Independent confirmation: asking to third parties considered independent and trustworthy to confirm some facts in which they have been involved. An easy example is asking to the bank to confirm the money present in the current account;
- Analytical review: this type of controls is performed by comparing data from different sources or different years. Into this category falls:
 - Trend analysis: checking if historical series show trends, and if there are spikes or differences not explained;
 - Ratio analysis: calculating ratios between two figures and checking for outliers;
 - Reasonableness analysis: checking if the figure analyzed is consistent with the other figures in the same document or report;
 - Scanning analytics: comparing auditor's expectation about a figure and compare with the actual figure. Calculating the variation and trying to explain it;
 - Regression: it is a statistical tool in which internal auditors may build a model to explain a figure, the so called dependent variable, through a list of independent.

Particular techniques can be used for antifraud audits. To tackle the fraud triangle, end period transactions have to be checked, because are the most probable to be fraudulently made by managers with under pressure to reach an objective. Related parties' transactions, unusual transactions and figures estimated are most the most common sources of fraud committed by managers.

Conducting tests efficiently may result difficult in situations where the items to be tested compose a rather big population. In those cases the internal auditor should consider using statistics and applying tests on a smaller sample.

There are two main sampling techniques:

- Judgement (or non-statistical) sampling. The internal auditor, using his or her experience and judgement, extracts the sample from a non homogeneous population by picking the items more likely to show certain characteristics. The result is a sample intentionally biased. The auditor wants to create a sample with common characteristics to run specific statistics. It is not possible to extrapolate conclusions valid for the population.
- Statistical sampling: the internal auditor defines the target population (that must be homogeneous this time) and the confidence level wanted from the statistics. The sample size is automatically given by specific mathematical formulas (Wilburn, 1984) and the sample is extracted randomly from the population. Statistics will give unbiased results that could be used to draw conclusion on the whole population.

All the tests and techniques above listed are the more traditional one, performed personally by the auditor.

More and more tests nowadays are performed through Computer Assisted Audit Techniques (C.A.A.T.), which run automatically thousands of those tests by relying on data withdrawn from databases. C.A.A.T. can enhance testing phase, but the internal auditor has to rely completely on the effectiveness and may not trust the automated test as much the one performed personally.

Test results and other material collected throughout the audit constitute audit evidence and should be conserved in proper working papers. Those documents conserve the basis for the audit opinion and the recommendation that will be issued at the end of the audit and will be precious for future audits²⁵.

²⁵ Further requirements on working papers are listed in the I.I.A. Performance Standard 2330.

Reporting

The results obtained from the audit work, mainly the audit opinion and the recommendations for the management, are issued through the audit report.

An important phase before the publication of the audit report is the wrap-up meeting. This step can be very stressful depending on the situation the auditor found. The wrap-up meeting can be much lighter if a sound relation with the manager has been built throughout the audit and if he has been informed constantly during the audit.

The final meeting is fundamental to explain and summarize the work done by the auditors and the main findings of the work. This is the occasion in which the manager can explain, clarify or justify some points of his or her system and give feedbacks to the internal auditors. The meeting provides many elements to write down the report draft that will include the agreed recommendations. It may seem counterintuitive that recommendations should be agreed with the management. It is instead fundamental that managers understand the changes proposed by the internal auditors and see the advices as issued by colleagues interested to the results. Recommendations imposed by a sort of authority might fall on deaf ears.

After all those steps, the assignment reports can be issued.

The report must be composed of the elements of the audit opinion, therefore mainly:

- The results of the control evaluation;
- The control culture;
- Key risks and issues;
- The adequacy and compliance of controls.

Recommendations include:

- The available options to modify controls or processes;
- Bad managerial practices that affect controls;
- The cost of poor control.

The report should contain actions plans to facilitate the work of managers.

Follow up

The reporting phase do not close totally the work of the auditors. The internal audit function should obtain assurance that managers do undertake the corrective actions recommended in the audit report. The nature, timing and extent of the follow up process depend on the significance of the issues emerged during the audit process but also on the resources of the internal audit functions. To

implement the follow up the internal auditors may inquiry periodically the management or perform additional audits on critical areas to check if recommendations have been fulfilled.

As we had the opportunity to see, the entire internal audit process presents some grey areas in which the expertise and the judgement, not regulations and neither best practices, drive the internal auditor to the right call.

Many studies have been done on Italian internal audit²⁶, but none on how the C.A.E. plan and conduct their audit work. One especially interesting aspect is represented by the tools and the tests used by the internal auditors during the field work. In the second part of this thesis we will investigate those aspects.

²⁶ Among others: Corbella, Pecchiari, 1999; Tettamanzi, 2000; Arena, Arnaboldi, Azzone, 2006; Selim, Woodward, Allegrini, 2009, PriceWaterhouseCoopers 2016.

Chapter 5: Empirical research

The aim of the empirical part of this thesis is to investigate the differences between the internal audit framework that has emerged from the literature and that has been presented in the previous chapters of this work and what internal auditors actually do in their companies.

The population chosen to conduct the research on is composed of the Chief Internal Auditors (C.A.E.) of companies that meet the following criteria:

- To be listed in a Stock Exchange;
- To have the headquarters in the North-East regions of Italy.

One more company has been added to the population, because it was considered comparable to the others even if it did not meet the two criteria: this company it was listed for a long period of time and then it withdrawn from the Stock Exchange, maintaining a solid internal audit function since today.

The research has been conducted via two means. The main source of data is composed of the answers to fifty-one questions of a survey sent directly to the C.A.E. of the companies under examination. The second source of information is given by five personal interviews with the C.A.E. This latter source obviously does not provide data that allow a quantitative research; however, they provided crucial understanding of the issue and many conclusions would not have been possible without them.

From a population of sixteen companies that matched the required characteristics, a sample of six C.A.E. answered to the survey. Every respondent asked to keep the denomination of the company confidential and not to provide information that could allow its recognition. For this reason, only aggregated data will be presented in this work, without description of single cases.

5.1 The survey

The survey has some peculiar characteristics that worth to be analyzed before starting to review the answers. It is composed of fifty-one questions, and can be divided into six main sections.

Section one provides a general description of the internal audit function.

Section two contains questions to localize the internal audit function in the corporate governance scheme and to investigate its relations with the other corporate governance bodies.

Section three investigates the audit work of the internal audit function and the main techniques adopted by the C.A.E.

Section four explores the relationships with management.

Section five provides an understanding of the internal control system in the companies composing the sample.

Section six probes the risk assessment process in the company.

The survey is composed of multiple choice questions, to facilitate and make faster its completion. For questions in which the C.A.E. had to make an evaluation, the possible answers have been chosen to be from 1 to 4, not to allow the interviewed to place a score in the middle and forcing him to choose a side.

Given the dimensions of this survey, only the most interesting questions have been analyzed.

Questions used for this work can be found attached in Appendix A.

The results of the survey are presented below. The structure of this analysis follows the one of the survey: the answers have been studied following the six sections already presented above.

The way of presenting the data has been taken from a very similar research done by Corbella and Pecchiari in 1999, in which questions are taken one by one or in groups and analyzed with the help of graphs and tables.

While other studies and surveys present in the literature explored the situation of internal auditing in Italy, none of those reviewed by the author focused on the audit techniques adopted by the C.A.E. For this reason, Paragraph 5.4 presented below represent in particular an original and innovative contribute provided by this thesis. The other sections, indeed, provide a picture indispensable to read that information.

5.2 General description of the Internal audit function

This section of the survey is dedicated to the general description of the function.

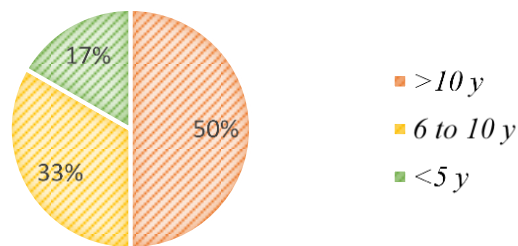
The aim of these questions is not only to form a general idea of the different internal audit functions present in the sample, but also to individuate some clusters in the sample. The clusters individuated will be explained at the end of this paragraph, with the help of a reassuring table.

Question 1: For how long does the I.A. function exist?

Question 2: Which events led to the introduction of the function?

Questions number one and two inquire the birth of the internal audit function in the sample.

AGE OF THE I.A. FUNCTION



TRIGGERING CAUSE

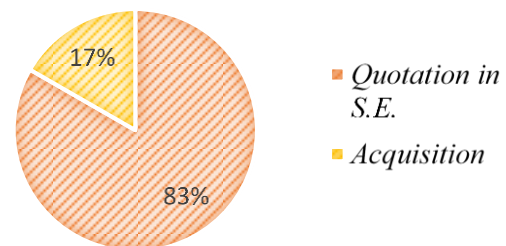


Figure 5.1: pie charts for questions 1 and 2 – Birth of the internal audit function. Elaboration of the author.

As can be seen from the graph in the right in figure 5.1, the 83% of the I.A. functions were born as a consequence of the quotation in a Stock Exchange (S.E. in the graph), despite for a case in which the company was acquired by a group that imposed the establishment of the function.

This result can be taken as the proof of the role of the legislator in imposing the institutions of an internal audit function. None of the six companies of the sample decided spontaneously to establish this institution, but were obliged by the comply or explain principle before the quotation in the Stock Exchange.

For what concerns the timing of the triggering cause, 50% of the functions exist for more than ten years, 33% from six to ten years and only one company established the function from less than 5 years. This information will be used to form the above-mentioned clusters.

Question 3: At which level is the function positioned in the group?

This question examines the positioning of the I.A. function inside the corporate governance scheme of a group. The I.A. function can be embedded in a group in three ways. Either at holding level, usually with a quite big function able to move and monitor the subsidiaries, at subsidiaries level, with smaller groups of internal auditors responsible for the single company, or at sub holding level.

This is a mere organizational choice, and no indication is provided by Italian laws or by the code of corporate governance.

In our sample, 83% of the companies maintained the I.A. function at holding level, monitoring the subsidiaries, and only the 17% place the function at single company level. No companies of the sample present the I.A. function at sub holding level.

One explanation to the pie chart shown in figure 5.2 could lay in the fact that the C.A.E. is considered the operative arm of the statutory auditors and of the C.F.O.²⁷ For this reason, the function should be

²⁷ Allegrini, 2011.

positioned in the organigram of the group as close as possible to the top management. Positioning the I.A. function closer to the board of directors of the holding company could also represent a further method for ensuring its independency.

I.A. FUNCTION LEVEL

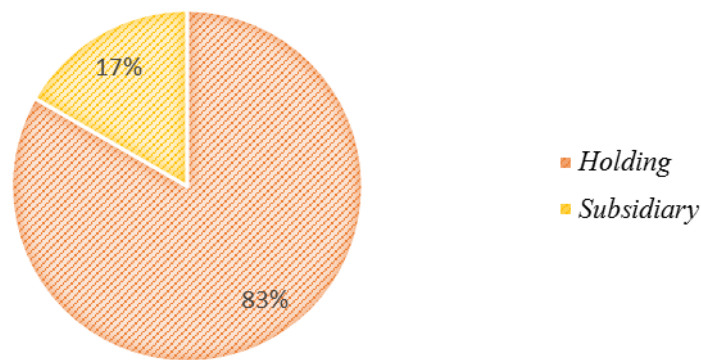


Figure 5.2: positioning of the I.A. function. Elaboration of the author.

Question 4: How many people are employed?

Question 5: How many people outside the company are employed on average in the I.A. function?

Question 6: Which are the professional profiles most represented in the function?

Question 7: On average, for how long do the components remain in the I.A. function?

Question 8: What is the annual budget dedicated to the function?

Questions from 4 to 8 investigate the resources at the disposal of the C.A.E. This information is important to evaluate the dimension of the functions composing the sample and the tools available to the C.A.E.

Question 4 and 5 regards the quantity of personnel employed in the I.A. function, C.A.E. included. The first regarding the internal employees, the second for the external ones. People with a part-time contract are counted as 0.5.

Results are included in Table 5.1 below, and will help with the formation of the clusters individuated. Question 6 asks the average background of the personnel, and the answer is no surprise. The personnel of the I.A. function is composed for the 50% of people with past experience in external audit firms, whereas the remaining 50% of people has a background limited to a degree in business or economics. Given the fact that internal audit shares many traits with external audit, this result was expected. However, during the interviews conducted with the C.A.E. it emerged that each one had experienced

external audit and employees with a degree in business or economics compose the audit team and are not the senior components of the audit team.

The turnover of the employees inside the function is inquired in question 7, and shows a surprisingly high rate in average. The 80% of the answers given to this question (one responder did not insert any answer) declared that personnel inside the I.A. function change each 5 to 8 years and only one respondent answered 3 to five 5. No companies retain an internal audit team for more than 8 years or for less than 3 years. This result is quite interesting, indicating that the team continues to change and to bring different experiences possibly in different areas of the company.

A vertical career inside the function, that would be signaled by higher number of years in the answer, have the advantage of creating people with more experience in internal audit. A horizontal type of career through different areas of the company, instead, has possibly the more important side effect to spread awareness throughout the company about what internal audit is and what it does. Those conclusions are in line with those individuated by Arena, Arnaboldi and Azzone (2006), that found in a similar study that some I.A. teams had a 3 years turnover in order to maintain a strict contact with the operations.

Question 8 asks for the annual budget available to the I.A. function. Data submitted by the respondents is to be intended net from the salary cost of the audit team and of the C.A.E.

Since a comparison of the absolute value would provide no clue for a comparison among the sample, the number has been divided by the Net sales of the respective company taken from the most recent financial statement available. The outcome is shown in per thousand.

The results are shown in the table 5.1 below, comparing all the companies composing the sample.

	A	B	C	D	E	F
Age of the I.A. function	>10 y	6 to 10 y	>10 y	6 to 10 y	>10 y	<5 y
Employees	8	2	8,5	4	4	1
External	0	0	0,5	1	0	2
Total H.R.	8	2	9	5	4	3
Budget/Net Sales	0,07 ‰	0,33 ‰	0,1 ‰	0,43 ‰	0,15 ‰	0,07 ‰

Table 5.1, data referring to question 1, 4, 5 and 8. Elaboration of the author.

This table highlights the creation of some groups among the sample. Companies A and C present solid I.A. functions, exiting from more than 10 years and composed by a conspicuous team based almost entirely only on people directly employed.

Companies D and E present similar numbers for the age of the functions and nearly half of the team members.

Company B present a small function, with composed only by two members, whereas company F is the most recent one, relying more heavily on the support of external personnel.

An explanation to the fact that long-standing I.A. functions do not rely on external personnel can be found in the particularly delicate task of the internal auditors: advising management and the bodies of the corporate governance framework about internal controls and more in general about how to reach the objectives. To accomplish this task extremely important are the relations that the I.A. function is able to create with whom have to receive these advices. There is no doubt that stronger relations can be established by an insider, and that this figure can be more trusted by the management rather than an external C.A.E.

For what concerns the expenditure, no real trend is shown by the data. Companies B and D are those with the highest budget to net sales ratio. Companies A and C seems to spend a relatively low amount of money for such complex and sound functions.

The average annual budget net of salary provided to the I.A. function in absolute terms is 92.000 €.

5.3 Positioning of the Internal audit function and relationships with other bodies

This section is composed of ten questions aimed at positioning the function inside the corporate governance scheme adopted by the companies composing the sample and aimed at discovering the relationships among the different bodies.

Question 9: From which body of the corporate governance framework does the I.A. function depends?

From the provisions of the Corporate governance code, the internal audit function is “subordinated to the board of directors” (Italian corporate governance code, p 32). Figure 5.3 shown below depicts a situation following quite correctly the provisions. Among the respondents, 33% declared that they are subordinated to the Board of directors, and the same percentage marked the chairman of the board. Those two results can be read as the same, signaling that two thirds of the sample follows perfectly the provisions.

One respondent marked the director responsible for the internal controls and risk management systems, and one the audit committee.

For what concerns those two last answers, further analysis has to be done. An I.A. function referring directly to the audit committee can be considered in line with the provisions only if the audit

committee is composed of members of the board. Unfortunately, the corporate governance report²⁸ of the company that marked this answer do not provide any detail in this regard.

Depending directly from the director responsible for risk and controls, instead, can be considered not in line with the provisions. It is important that the whole board of directors is considered the body the C.A.E. has to refer to. Only in this case there is the assurance that also the minority shareholders are informed of the work done by the function, and can ask it for specific controls or audits. Depending from the audit committee has to be considered a second best option.

DIRECT REFERRING BODY

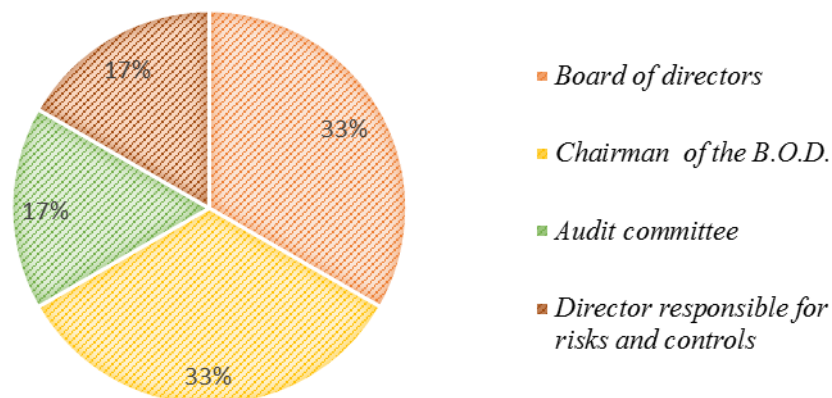


Figure 5.3: data from question 9. Elaboration of the author.

Question 10: With which bodies is there a closer and more frequent contact?

This question asks how strict are the relations between the C.A.E. and the other bodies composing the corporate governance framework of the company. The respondents were asked to choose a score from one to four, with four standing as strict and frequent relations and one as weak relations.

Table 5.2 below explain the results.

²⁸ “Relazione sul governo societario e gli assetti proprietari” is the Italian translation.

Bodies	Mean	Variance
Board of directors	2,17	0,97
C.E.O.	3,00	1,20
Chairman of the B.O.D.	2,50	1,90
Director responsible for risks and controls	3,67	0,27
Audit committee	3,20	0,70
Board of statutory auditors	3,00	0,40
Supervisory body 231/2001	3,33	0,67

Table 5.2, data referring to question 10. Elaboration of the author.

As can be seen, the stricter relations, represented by the highest mean of 3.67, are with the director responsible for risks and controls. The very low variance demonstrates that almost all the respondents were in agreement. This result is explained by the fact that this director can ask to the internal auditors several services and reports about the state of the internal controls and risk management systems, monitored repeatedly by the I.A. function. This director and the C.A.E. should work frequently together. The monitoring of these two systems done mainly by the internal auditors should provide new idea and suggestion to this director to enhance the other steps individuated by the C.O.S.O. The highest variance is present with the Chairman of the board of directors, that clearly has different roles among the companies.

One unexpected result was the mean of 2.17 scored by the board of directors, the lowest among all the actors. This can be explained by the fact that the boards rely heavily on the director responsible for risks and controls, and do not enter in detail about the internal control and risk management systems.

Question 11: Which of these mechanisms are most important for the transmission of information within the internal control system?

It is now interesting to discover the methods through which the I.A. function enters in contact with the other bodies. Question 11 found that the most effective way was by scheduling periodic meeting with the different bodies, with a mean of 3.5 out of four. Slightly below scores the approval of the audit plan and the preparation of reports by the C.A.E. of reports sent to the different bodies. The least used method to enter in contact with other bodies, with a mean of 2.83, is through cross memberships, in which different actors meets as members of a body.

One of the most common opportunities for cross memberships is provided by the supervisory body ex Legislative Decree 231 of 2001, since its composition is not indicated by the legislator.

Question 12: Who nominates the responsible of the I.A. function in the company?

In this case every respondent was compliant with the provisions of the corporate governance code by choosing board of directors (with the favorable opinion of the other member of the system of internal controls).

Question 13: Who are the addressees of the periodic reports?

Question 14: Does the C.A.E. think that the reports are considered by the recipients?

Question 15: Does the C.A.E. take part to the controls and risks committee's meetings?

Question 16: What kind of relation does exist between the C.A.E. and the supervisory body ex D. Lgs 231 of 2001?

Question 17: What kind of relation does exist between the C.A.E. and the person responsible for the preparation of the corporate financial documents ex L. 262 of 2005?

Question 18: How often is the C.A.E. consulted in the definition of the business strategies?

Question 13 aims to identify the addressee of the reports created by the C.A.E., other strong signal of the relations among the bodies composing the corporate governance structure.

Figure 5.4 below reports the results.

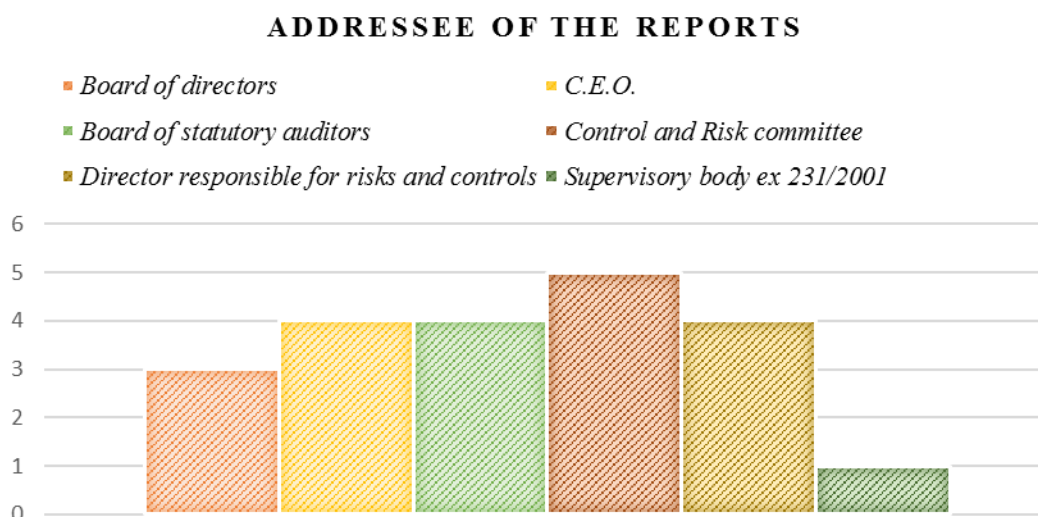


Figure 5.4: Addressee of the reports of the C.A.E. Elaboration of the author.

The results show that the reports of the I.A. function are sent to many and diversified bodies composing the corporate governance framework. This graph has to be read together with the results coming from question 14, in which 83% of the respondents declared that in their opinion the reports are taken into consideration by the addressee and carefully examined. This data picture a situation in which the monitoring and advising role of the internal audit function is recognized by the other bodies. Only one respondent answered that the reports are considered superficially by the other bodies.

The spike in figure 5.4 showing the reports sent to the control and risk committee and representing strong relations with the I.A. function, are confirmed also by question 15: 66% of the C.A.E. stated that they always participate to the meetings of the committee. One respondent declared to attend more than 50% of the times and the last declared less than 50% of participation.

In figure 5.4, the low score of the supervisory body ex D.L. 231 of 2001 can be explained by the fact that often the C.A.E. is member of this body. Question 16 confirms this theory. 83% of the C.A.E. are members or chairman of this body.

Who benefits from the advices of the I.A. function is also the person responsible for the preparation of the corporate financial documents, imposed to the companies by the Law 262/2005. Question number 17 asks how frequent the contacts between the C.A.E. and this person are. Among the respondents, 50% declare to have frequent contacts with this person during the period in which the financial statements are prepared. Two respondents answered to have only limited contacts and one answered to have no contacts with this person.

Question number 18 inquiry how trusted is the C.A.E. by the board of directors and by the top management of the company, by asking if it is consulted for the strategic decisions of the company.

HOW OFTEN IS THE C.A.E. INTERPELLED FOR STRATEGIC DECISIONS

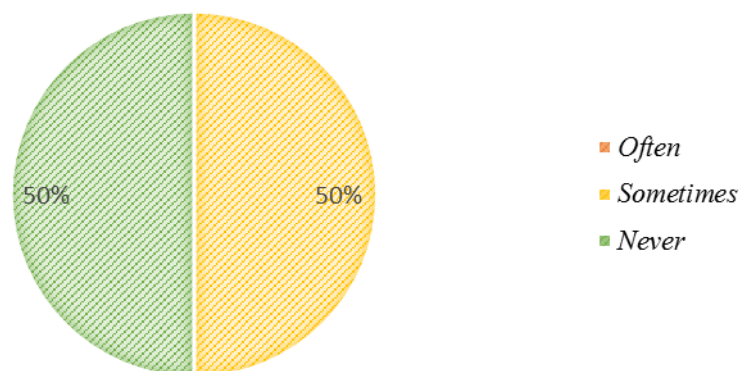


Figure 5.5: how often is C.A.E.'s advices asked for strategic decisions. Elaboration of the author.

The result shows that the C.A.E. are considered important for long term strategic decisions in 50% of the companies of the sample.

Basing on what the theory suggests, the insights of the internal auditor over the system of internal controls and over the risk management system should be recognized as strategic by the board of directors and the top management, but this is not the case in half of the companies. Evidently, some companies approach the reports issued by the internal auditors as they are, not really extracting possible interventions that could be done mainly on the system of internal controls.

Overall, concluding the analysis of this section composed by questions regarding the positioning of the internal audit functions, some conclusion can be drawn. It emerges a picture in which companies organize the corporate governance system slightly differently among them, with different role and weight assigned to the board of directors, its chairman and to the directors responsible for risks and controls. By the way, law provisions are in general followed.

The fact that the internal auditor is dependent from different bodies could contribute to the general sensation of confusion around this figure.

The advices of the internal auditor, that this survey found to be mostly issued via formal reports sent, rather than with more informal means, are considered precious by the other bodies and are taken in serious consideration.

The use of reports is suggested by all the bodies setting the standards for the internal audit profession, because they are formal, unchangeable, with a similar structure that is always repeated and so easier to understand. Besides this official mean, Pickett (2010) reminds how important the relationships built by the internal auditor are important for the success of the function. During the interviews conducted with the C.A.E., it emerged how important are the transversal skills owned by the members of the audit team to facilitate the issuance of the suggestions contained into the report. This is the scope of the wrap-up meeting that has been described in detail in Chapter 4.

The reports may provide strategic suggestion to enhance the system of internal controls or the risk management system, but only in 50% of the cases those reports do trigger a response by the top management to ask further contribution to the I.A. function.

By following the three clusters individuated in table 5.1, the results in this section were similar among the companies, except for the company with the smallest I.A. function in which the C.A.E.'s report are less considered and he participates to the meeting with the control and risk committee only 50% or less of the times, signaling that smaller function could be perceived as less important from the other bodies composing the corporate governance framework.

5.4 Audit plan and audit techniques

Section five of the survey directly refers to Chapter 4 of this work, and is intended to discover which differences are present between the theory coming from the literature and the practice. Questions from 19 to 21 refer to the audit plan. Questions from 22 to 31 refer to the audit techniques.

Question 19: How often do all the main business processes receive an audit?

Question 20: How much importance does the following elements did receive during the preparation of the last audit plan?

Question 21: By whom is written the audit plan?

There is no right answer to question 19: it depends on the resources available, the dimension and complexity of the company or of the group and the level of materiality set by the internal auditor. With a low level of materiality there will be more processes to control, therefore the timing for an entire cycle of audit will expand.

As expected, the answers given differentiates. In 50% of the cases, the timing for an entire cycle of audit is from 3 to 5 years, in 33% of cases more than 5 years and in 17% case is less than 2 years.

During the interviews, however, the auditors stating that a complete cycle lasts 5 years ensured that riskier processes or those which reach materiality determined materiality levels are checked more often. This condition is fundamental to assure that core controls are functioning and that the most important processes can be considered safe according to the internal auditors' judgement.

Question 20 inquiries how important the five main objectives that internal audit has to achieve through its activities, as for the I.P.P.F. standard 2120. Table 5.3 below summarize the answers gathered.

Objectives	Mean	Variance
Compliance	3,17	0,57
Operations	3,17	0,57
Maintaining assets value	2,50	0,70
Reporting	3,17	0,57
Strategy	1,83	0,57

Table 5.3: Data referring to question 20. Elaboration of the author.

As we can see, the average audit plan is focused on the compliance of the company with the applying laws, on the efficiency and effectiveness of the operations and on the reliability of financial and

operational information. The safeguard of assets scores the fourth place and the achievement of the company's strategic objectives is last point taken into consideration.

These results fit very well with those obtained in the previous section: the reports issued by the internal auditors could have a strategic importance for what concerns advice about the system of internal controls and the risk management system, but only rarely such an important response is triggered.

We also immediately see how the three objectives mostly included in the average audit plan are those matching with the C.O.S.O. internal control framework steps analyzed in Chapter 3.

For what concerns who writes the audit plan, question 21 finds all the respondents in agreement and compliant with the provisions in saying that the audit plan is written by the C.A.E. and approved by the Board of directors and other corporate governance bodies.

Question 22: How much do the following characteristics of a process weight into the creation of the audit plan?

For what concerns the elements that mostly affect the construction of the audit plan, table 5.4 below shows the results.

	Mean	Variance
Risk	3,83	0,17
Materiality	3,50	0,30
Dimension of the process	2,83	0,97

Table 5.4: Data referring to question 22. Elaboration of the author.

Risks is the leading reason to include a process into the audit plan with almost the maximum score, followed by the materiality. The least affecting element to affect the audit plan is the dimension of the process, intended as people employed. This latter result could be explained by the fact that even small processes could be potentially dangerous if they present high risk and they are material.

Stressing more risk and materiality is in line with the principles of internal auditing: risk is the likelihood of an event to happen, and materiality, more than the dimension of a process, is an indicator of its impact.

Question 23: In average, how much does an audit last?

Question 23 starts approaching the audit process.

As we can see in figure 5.6 below, there is a high variance in the answers and different behaviors are shown. Pickett (2010) recommend an average duration of an audit of three weeks or one month to complete all steps analyzed in Chapter 4 and that will be tackled with the next question.

AVERAGE AUDIT DURATION

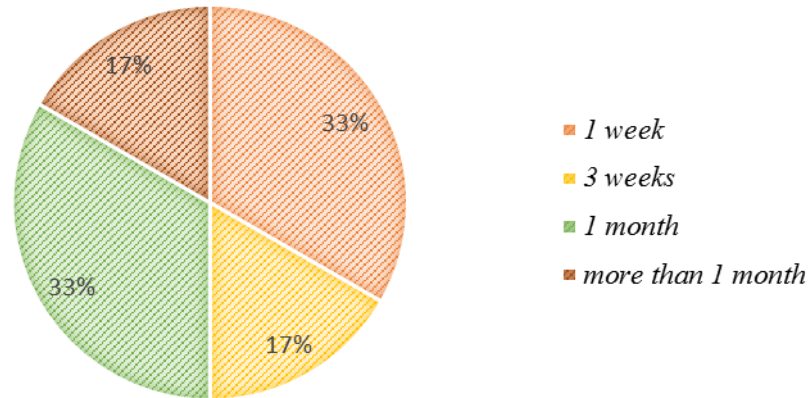


Figure 5.6: Average audit duration: Elaboration of the author

All the answers are sticking with the theory. The only outlier is represented by the C.A.E. of company B, with the smallest internal audit function, that spend in average only one week for the average audit. This timing seems quite short to go through all the steps present in the theory.

Question 24: How much time-absorbing are the following activities during and audit?

This question helps to understand how much time do the steps identified in Chapter 4 require during an audit, in average.

Results are presented in table 5.5 below.

Phases	Mean	Variance
Preliminary survey	2,00	0,80
Engagement programme	2,50	1,10
Field work	3,33	0,67
Reporting	2,83	0,17
Follow-up	1,83	0,57
Archiving	1,33	0,27

Table 5.5: Data referring to question 24. Elaboration of the author.

The engagement programme scores the mean value of 2.5, but has the highest variance, present also in the preliminary survey. This can signal that the auditors have different opinions about how much time should be spent in this phase into the preparation of an audit.

Field work, as expected, has the highest mean. It is indubitably the most time-consuming phase, in which all the data to form recommendations is collected.

High scores are present also for the reporting phase. The interviewed chief internal auditors put a lot of effort and time in the reporting and issuing recommendation. As already explained for precedent questions, reporting is crucial to achieve that the message is well understood by managers. Reporting phase also comprehend the above-cited wrap-up meeting, that must be prepared carefully. A very low variance confirms that the respondents agree.

Following up and archiving are considered faster activities.

Question 25: Before starting an audit, does the C.A.E. always control the design of the controls over a process?

Among the respondents, 50% declared to engage this preliminary control always, 33% do this only sometimes and 17% of the sample never does it. The answers do not follow the clusters individuated, indicating that this is a precise choice of the C.A.E. and it is not related to the size or budget of the function.

This is a basic control done, that can be avoided for processes and controls that remains unchanged over time, but that is crucial not only in the case of endogenous changes, but also if exogenous elements interfered with a process or a control.

Question 26: During field work, how often does the C.A.E. uses the following audit techniques?

With this question, this work enters right at the heart of the techniques adopted by the C.A.E., that are required to assign a score from one to four to the frequency with which they use the most common audit techniques. Results are presented in table 5.6.

Techniques	Mean	Variance
Physical count	2,17	0,57
Interviews	3,83	0,17
Surveys	1,17	0,17
Reperformance	1,17	0,17
Confirmation letters	1,50	0,30
Reconciliations	2,17	0,17
Recalculation	2,00	0,40
Trend analysis	2,33	0,27
Documentation sampling	3,67	0,27
Regressions and statistical models	1,17	0,17

Table 5.6: Data referring to question 26. Elaboration of the author.

The results are interesting.

Physical count of objects scores right below the average value for this sample, that is 2,5. This result is explained by the fact that this technique is adopted only during audits in which counting is fundamental, as the control of the warehouse stock, and therefore it is not used in every audit.

Interviews with the personnel are conducted in every audit for the 83% of the C.A.E. of the sample. This is the most used instrument, because it is fast and it provides a precise picture of how much the employees understand the controls they are applying and if the controls are flowing as from the design.

Surveys, reperformances and confirmation letters are instruments almost never used by the C.A.E. composing the sample, mostly because they are very time-consuming.

Reconciliations and recalculations are more used, but in less than half of the audits.

Another spike is found in document sampling. In this case, it is used in every audit for the 67% of the sample. It is one of the most common testing tools for auditing in general, therefore the result is not surprising. Many C.A.E. confirmed during the interviews that internal auditing is a job characterized by a lot of paperwork examination; at first sight, this could seem an old or ineffective technique. Instead, auditors often use from the documents produced in the process or from the controls because they are a standardized source of information that can be easily compared to find errors. Unfortunately, this is also a quite long process if the auditor requires a sound sample to have the reasonable assurance that no errors or problems are present.

A surprising low result score trend analysis and statistical techniques. The I.A. functions of the companies composing the sample do not use quantitative techniques, and stick to the more “traditional” and hand based techniques, rather than using quantitative instruments.

The low variance shown in every technique under examination demonstrate how there is no difference in the work of the internal auditor depending on the size of the company or of the function. This fact is quite surprising: despite the differences among the I.A. functions composing the sample, they all use the same techniques in average.

Question 27: In percentage, during an audit, how often is a walkthrough conducted?

This question tackles directly the walkthrough technique. The average rate with which this activity is performed right at the beginning of an audit is 80%, confirming the importance of this tool, that for Pickett should always be performed to form a general idea of the process.

Question 28: During antifraud test, how often are the following techniques used?

Antifraud audits are an important part of the tasks of the I.A. function.

Figure 5.7 below presents the results

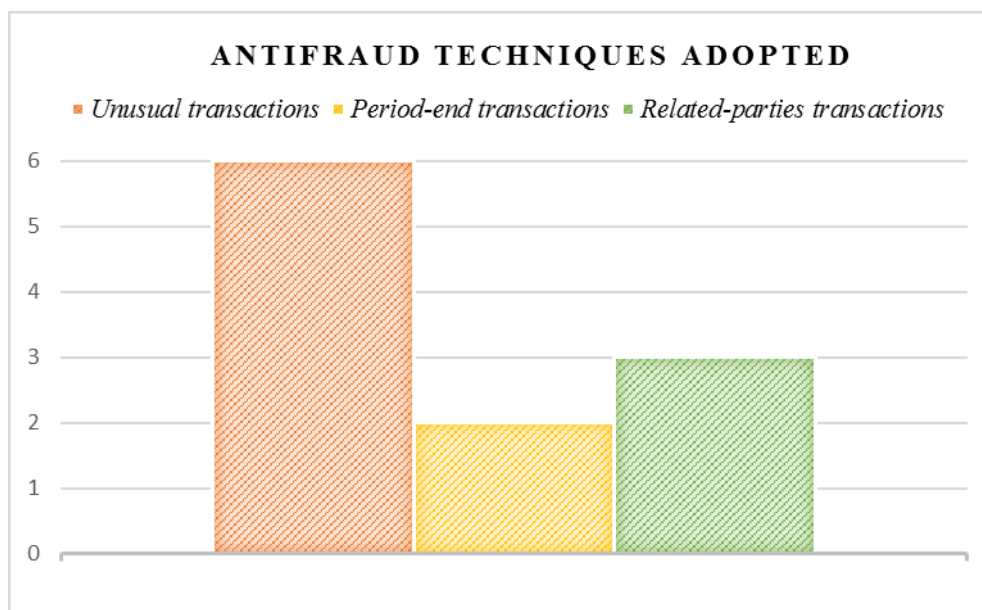


Figure 5.7: Results relative to Question 28. Elaboration of the author.

The fraud triangle, presented in Chapter 3, states that there is the possibility of a fraud whenever three conditions are met: pressure, opportunities and justification of the fact by the manager.

As we can see from the graph, the controls over unusual transactions is a technique adopted by every respondent. It may be considered one sound way not to go in detail with the three elements of the triangle.

Only half of the sample controls related-parties' transactions, that should tackle the opportunities of managers and the 33% of the sample checks period-end transactions, controlling over the pressure to reach the objectives.

No C.A.E. in the sample controls management estimation. This fact could be justified by the fact that managers calculations are considered generally correct, or by the fact that they require a level of expertise about the operations not in possess of the C.A.E.

Question 29: Through which documents are audit results archived?

From the answers to this question, the most used ways to perform this task are with the help of photocopies, with 83% of the C.A.E. of the sample always using this instrument, and through working papers, used in every audit used by the 67% of the respondents.

Archiving the documentation after an audit is fundamental to keep track of the work done. The following audit over the same process will be based on the results of the previous audits conducted, so clear documentation of the main tests and results have to be recorded.

It is important to signal that working papers and photocopies are not substitute, but are two instruments with a different scope. While the first is a summary of the whole audit and of the main findings, the second is useful to record the proofs of tests done.

Question 30: In percentage, how many audits do receive a follow-up?

After an audit is concluded, the last step to proceed with is the follow-up. The sample average for who conducts a follow-up after an audit is 78%, and the answers do not follow the clusters individuated. This result was expected, and could be justified by the fact that positive audits that do not came up with recommendations does not need a follow up.

In this section, we examined the composition of the audit plan of the I.A. function composing the sample, which audit techniques are more used and if the steps identified for the theoretical audit are followed.

For what concerns the composition of the audit plan the answers were mostly aligned with the theory, apart from the fact that the objective recommended by the I.I.A of safeguarding assets value is considered less important. The small contribution perceived by the C.A.E. for what concerns strategic changes triggered by their reports is confirmed also in this section.

About the audit techniques, the results do not deviate much from the theory, but there are a couple of details to highlight. Firstly, the low usage of mathematical and statistical techniques is a characteristic present in all the companies composing the sample. This can be explained by the fact that the theory is based on the experience of huge companies and therefore more complex and richer I.A. functions, that allow the usage of those instruments. For example, computer assisted audit techniques presented in Chapter 4, able to run thousands of tests on databases are probably needed only by few I.A.

functions worldwide. But the almost absolute absence of quantitative techniques used by the C.A.E. was unexpected. Only trend analysis, which are the easiest quantitative instruments found in the theory are used by almost the 50% of the sample.

Secondly, antifraud activities highlighted within question 28 seems weak. The literature reviewed about internal audit antifraud techniques explicitly suggest checking managers estimations by simply asking to how the output figure was figured out, and the reason why no C.A.E. in the sample does this apparently simple check is unclear. Furthermore, controls over period-end transaction, a technique that can be used to discover if manager under pressure committed fraud, are carried out only by the 33% of the sample, signaling that C.A.E. base their antifraud activity checking almost solely unusual transactions.

The results were comparable among the sample for every question, with no particular deviation of one company from another. One outlier is worth to be analyzed. The audit duration of one week declared by the C.A.E. of company B that seems excessively short, compared to the theory and to the rest of the sample.

5.5 Management relationships

Question 31: How does the C.A.E. considers relations with the management?

Question 32: Which are the major sources of resistance from the management?

Question 33: In the opinion of the C.A.E., management consider the I.A. function as value generating?

Those three questions deal with the relationship with managers and possible resistance reasons.

In question 31, the 83% of the sample stated that the management respects and trust the I.A. function and its work. Only one respondent signals minor contrasts with the management, the C.A.E. of company B.

Question 32 asks which are the main sources of resistances from the management. Figure 5.8 below summarizes the results.

MAIN SOURCES OR MANAGEMENT RESISTANCE

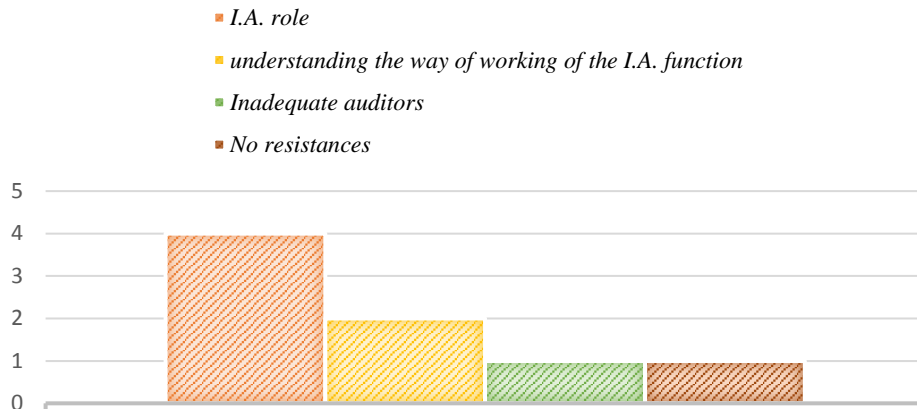


Figure 5.8: results of question 32. Elaboration of the author.

The major source of resistances is represented by the weak comprehension by the management of the role of the internal auditor. This result highlights the importance of the audit charter to spread information about the still quite blurred role of the internal auditor. This conclusion is supported by the results of question 33. Among the sample, 50% of the C.A.E. declare that management considers the function as generating value, whereas the other 50% state that the function is considered merely necessary for compliance. For what concerns the clusters individuated in table 5.1, both companies B and F, considered the smallest and the newest functions created, both are not considered by managers as value generating. The third one is represented by company C, one of the biggest of the sample.

The conclusions drawable from this section are very important. Management respect and trust the internal auditor and its advices, but has not a clear idea of what it represents and what it does.

The I.I.A. is following a good path by asking to the internal auditors to issue the audit charter, that should allow everyone inside the company to acquire information about the I.A. function. This simply seems not sufficient. One more hope for this problem is the horizontal turnover highlighted in question 8. The possibility that different people can move through the company and join the audit team for some years can represent a way of bringing new skills to the team, but also to spread knowledge about the I.A. function.

Finally, the value generation issue of internal audit function is really difficult to tackle, because no real instrument can be individuated to evaluate the value generation of this thesis. The fact that C.A.E. of company A, D and E declared that managers perceive the function as value generating could be as

sign that a sound and robust function operating for enough time is able to establish more and more positive relationships with the management that can greatly appreciate their advices.

5.6 Internal control framework

Question 34: How much importance does the following elements of the internal control system have in the company?

Question 35: Managers are aware of their role inside the internal control system?

Those two questions regard the internal control framework in the companies composing the sample. Question 34 asks how are developed the different elements of the C.O.S.O. internal controls framework. During the interviews, the C.A.E. confirmed that they all adopt this framework.

Data from question 34 is presented in Table 5.7 below.

Elements of the Internal control framework	Mean	Variance
Control Environment	3,17	0,57
Risk assessment	2,50	0,30
Control procedures	2,67	0,27
I.T.	3,17	0,57
Monitoring	2,67	0,27

Table 5.7: Data referring to question 35. Elaboration of the author.

As shown in the table, a very high result is scored by control environment and I.T., whereas risk assessment, control procedures and monitoring scores the same result as the mean or just above. Variances are low, signaling that the C.A.E. of the companies composing the sample share a common perception about the importance of the various elements of the internal control system.

The average result of control procedures has to be read together with the results coming from question 35, asking to the C.A.E. if managers, that should represent the first and second line of defense against risk for the Italian code of corporate governance, are aware of their role inside the internal control system. By choosing from Totally aware, Aware but not totally, Limitedly aware and Not aware, 50% of the sample stated that their managers seem aware but not totally of their role and the other 50% declared that their managers seems only limitedly aware of their role.

With managers only mildly conscious of their tasks, safe and sound control procedures cannot be performed.

It is quite surprising to see the monitoring element of the internal control framework, that the internal auditor does not perform alone but as a major actor, not highlighting a higher score. This can be due to poor attention shown by other actors of the corporate governance system, as the board of directors. Scores regarding risk assessment have to be seen together with the results from the following paragraph.

Finally, it is important to highlight that the auditor of company F, with the small and relatively newly introduced I.A. function, marked much lower scores in question 34. This can prove that a longer work done by the auditors have a tangible effect on the internal control system.

5.7 Risk management system

Question 36: Does it exist a shared method to prioritize risks for the whole company?

With this question, the analysis of the risk management system begins.

Half of the respondents answered that the whole company uses the same method, during the interviews identified as the risk matrix by every C.A.E., to prioritize and classify risks; the other half of the sample, instead, stated that every business unit or company of the group uses a different method. Obviously, the solution in which a unique and standardized matrix is used is advisable, but it is not always possible. Groups with a high degree of differentiation could find more difficulties to share a common risk matrix.

Question 37: During the risk assessment phase, which typologies of instruments are used?

This question regards the typologies of risk calculation techniques adopted by the C.A.E.

The results are presented below in figure 5.9.

RISK CALCULATION TECHNIQUES

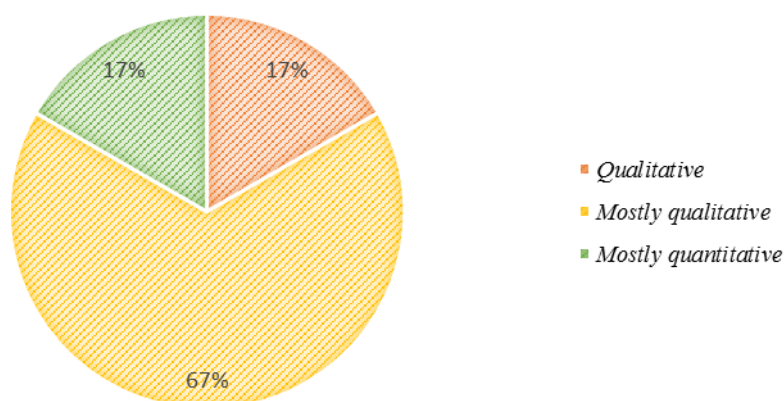


Figure 5.9: results of question 37. Elaboration of the author.

The usage of quantitative techniques is not spread, and only one C.A.E. report to make a prominent use of them. Qualitative methods, therefore based on the auditors' judgement are more spread, because easier and faster, but generally more imprecise.

Question 38: How is materiality calculated by the I.A. function?

A similar question is presented in respect to the calculation of materiality, and the results are exhibited in figure 5.10.

MATERIALITY CALCULATION

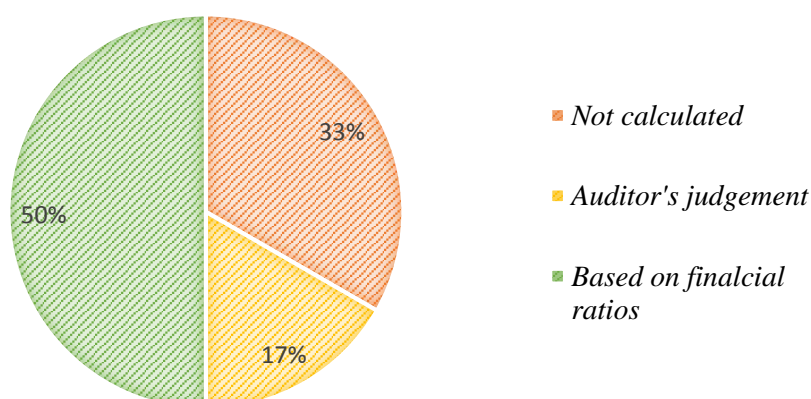


Figure 5.10: results of question 38. Elaboration of the author.

Only the 50% of respondents answered to apply a percentage to different balance sheet items in order to calculate materiality. The 17% bases its calculation on its own judgement and the 33% declare not to calculate materiality during the risk assessment phase.

Also for what concerns materiality calculation, the interviewed internal auditors do not use often quantitative instruments, but instead rely abundantly on their own judgement.

The conclusion to this section provides a picture in which the I.A. functions are generally not using quantitative methods to estimate materiality threshold and assessing risk. For what concerns the clusters, companies A and C, the biggest for number of members of the I.A. function, do present a shared risk matrix for the whole company and use the simple method of linking materiality calculation to balance sheet items. However, even for those two functions, risk is calculated using solely or in majority qualitative instruments.

Not relying on quantitative instruments can be justified by a lack of skills of the audit team or simply by C.A.E. believing their professional judgement is sufficient to assess risk and calculate materiality.

Chapter 6: The Italian Space Agency Experience

As anticipated in the introduction, this work presents also a parallel case of internal auditing, represented by the experience of Mr. Massimo De Angelis inside the Italian Space Agency (I.S.A.). The comparison between internal audit in public companies and state-owned organizations is extreme and not easy to conduct, but there are similarities that can be interesting to deepen and important information can be extracted for the conclusions.

It was possible to make a comparison between internal audit and an akin figure due to the background of Mr. De Angelis as internal auditor. Unfortunately, it was not possible to submit to him the same survey sent to the C.A.E., due to the massive difference among the I.A. function and the similar body that will be presented below. Therefore, this chapter will not be able to compare audit techniques performed. Instead, its purpose is to present a body similar to the function described in the previous chapter of this work which tried to transfer some internal audit characteristics into a state-owned organization. All information provided about the activities of this body in the I.S.A. derives from the interview had between the author and Mr. De Angelis.

6.1 The independent performance assessment body

The Italian Space Agency is a state-owned entity based in Rome. Its activities range from space science, satellite technologies to the development of mobile systems for exploring the Universe. This work focuses on the independent performance assessment body²⁹ of the I.S.A., the closest function that can be found in state-owned entities to the internal audit function. This body was imposed to the entities with the Legislative Decree 150 of 2009, and is entitled with tasks very similar to those of an internal audit function:

- Monitoring internal controls and reporting about it at least once a year and communicating criticalities found;
- Overseeing and evaluating the performance of managers and personnel and communicating the main results to the president of the entity;
- Overseeing that the entity is in compliance with the applicable laws;
- Controlling that no fraud is committed, ex Law N. 190 of 2012;

²⁹ Organismo Indipendente di Valutazione delle performance (O.I.V.) is the Italian name.

- Overseeing the transparency of information issued by the entity, ex Legislative Decree 97 of 2016;
- Controlling that the entity is considered in compliance with the transparency requirements, meaning that information about the performance of the entity and its management, resources available and every other significant aspect of the organization shall be easily available to every citizen.

The independent performance assessment body is composed of one or three members, appointed by the president of the entity, from which the body depends directly, without intermediaries. The members shall remain in office for a maximum of three years, with only one possibility of reappointment.

Legislative Decree N. 150 of 2009 recommends that the appointee have experience in management of public entities, valuation of personnel and of performances of public entities.

As can be clearly seen from the law provisions, the independent performance assessment body in state-owned share a lot of characteristics with internal auditing.

In our case, the body assesses the performances of the various divisions of the entity and of their managers by using actual audit methods. This is not a shared characteristic of the independent performance assessment body of state-owned entities, instead it is a peculiarity of the I.S.A. made possible thanks to the background of Mr. De Angelis.

The next paragraph will describe the activities done by the body examined that are similar to those performed by an internal audit function.

6.2 The I.S.A. case

In the Italian Space Agency, the independent performance assessment body is composed by three people: one person with legal background, that also acts as chairman, one with administrative background and one with experience in performance assessment.

The body has strict relations with the president of the entity, with the board of auditors³⁰ and with the board of directors. Those actors not only receive the annual report on the activities carried out by the body but can also require the assessment of specific internal controls or divisions' performances.

It has an audit plan, self-written and approved by the board of directors.

³⁰ Collegio dei revisori dei conti in Italian.

Moving to the activities done by the independent performance assessment body, the most important processes of the space agency have been mapped, and the intention is to complete this task for every process.

In terms of time used by the different activities, 50% of it was spent in compliance over transparency and antifraud, 20% in assurance by fulfilling the requests came from the other bodies and 30% in audit activities done to assess the performances of the divisions of the entity and the controls over it. Through assurance activities, this body is able to provide strategic advices to the president and the top management of the entity about how to enhance performances and internal controls, and its advices are taken in serious consideration.

For what concerns risks, the independent performance assessment body valuates risks linked to its core activities: mainly transparency and frauds. The framework used is the above mentioned E.R.M. provided by the C.O.S.O., fed with categorized risks coming from the Italian antifraud authority³¹. Risks assessment is conducted using mainly qualitative instruments. Once risks have been valuated, internal controls are verified in order to check if they are sufficient to reach the tolerance limit, concept already explained in Chapter 2.

The body has no role in evaluating the efficiency of the entity and possible cost savings of the divisions. In state-owned entities, especially in the case of a so prestigious one as a space agency, the effectiveness is way predominant over the efficiency.

It is important to highlight that this case is not unique in Italy: a similar situation is present also in other entities³², but it is certainly not common.

From the interview with Mr. De Angelis, an interesting scenario emerged for the evolution of internal audit profession in Italy. The I.S.A. provides an example in which methodologies peculiar of internal audit have been used in a body that has many characteristics in common with an I.A. function.

A future intervention of the legislator could enlarge in each state-owned organization the duties of this body with the main activities performed by internal auditors in public companies, following the I.S.A. model. This would provide those entities with capabilities already in possess of internal auditors, and standardize the methodologies and techniques adopted to carry out its tasks in a more effective way. Furthermore, new emphasis could be placed on the efficiency of processes, rather than only on effectiveness.

³¹ Autorità Nazionale Anti Corruzione (A.N.A.C.) in Italian.

³² Also the C.N.R, Consiglio Nazionale delle Ricerche in Italian, presents a similar situation. (Consiglio Nazionale delle Ricerche, 2013).

Conclusions

This work presents the state of internal audit functions of a sample of six companies located in the North-East of Italy.

To achieve this goal, international literature has been reviewed and a brief summary is presented below.

To explain the internal audit function, this work has been structured in levels.

Firstly, the corporate governance frameworks that applies for U.K. and Italy has been summarized and compared.

Secondly, the theory for risk assessment and internal control systems has been analyzed, focusing particularly on the C.O.S.O. frameworks, world famous guidelines for those topics.

Finally, internal auditing has been described, from the definition, through the professional principles and main objectives, to the audit field work and the main audit techniques that can be adopted by an internal auditor.

For what concerns the empirical part, the methodology to collect the data via a survey sent and interviews conducted with the C.A.E. of the sample have been explained, and successively the results of the research have been presented and analyzed.

The main conclusions drawn follows.

The positioning of the internal audit function inside the corporate governance framework and the relations established with the other bodies of the framework follows almost completely the provisions from the Italian corporate governance code with some minor deviations, confirming that the comply or explain principle is enough to encourage companies to respect the regulations.

The function is considered useful and is trusted by top managers. Communications is conducted as from the literature, with official reports issued the different bodies of the corporate governance framework of the company that are read and taken into consideration. In half of the companies composing the sample, the reports do trigger sometimes strategic intervention over internal controls and risk assessment; in the remaining half of the sample, there is no strategic contribution by the function. During the interviews conducted with the C.A.E., it emerged the importance of transversal skills to build significant relations with the auditee and top management to be sure that advices issued are received proactively.

Audit plan and techniques have then been analyzed, and interesting results emerged.

Among the main objectives identified by I.P.P.F. Standards 2120.A1 and 2130.A1, internal auditors are very focused over compliance with applying regulations, effectiveness and efficiency of

operations and integrity of financial information issued by the company. Less effort instead is being put into asset safeguard and strategic advices over the internal control and risk assessment systems. For what concerns audit conducted, the respondents follow the main guidelines coming from the literature about audit timing and the general scheme in which an audit is divided, with slightly differences in opinions present mostly in the preparation phase of an audit, during the preliminary survey and the preparation of the engagement programme. There is a general agreement over the importance of reporting phase and about follow-up.

Particular focus is being put into examining audit techniques used by the internal auditors composing the sample; the techniques used partially follow what the literature suggests as the most effective instruments to collect audit evidences. In particular, walkthroughs are almost always used to figure out how a process works, and interviews with the employees and managers applying internal controls appears to be considered very effective to assess the quality of internal controls, together with document sampling, confirming that internal auditing is still a job composed by a lot of paperwork. Surprisingly, mathematical-statistical techniques are only rarely used by the internal auditors composing the sample, a full deviation from what the literature suggests. This result can be partially explained by the dimension of the examined companies, or by a lack of skills in the audit teams. Quantitative instruments are used only by less than half of the sample also for what concerns risk assessment and materiality calculation.

Also in respects of antifraud techniques what has been declared by the respondents deviates from the literature, with fundamental controls over management estimation that are not conducted by any of the C.A.E.

Results for audit plan and techniques shows no differences among the sample, indicating that no real difference in the activities conducted is made by the dimension of the function or of the company.

For what concerns the relations with managers, data shows that the I.A. function is overall respected and accepted; however, there is a widespread sentiment of confusion about the role of the internal audit function inside the company from the management, that brings to mild resistances towards the internal auditors.

The value generated by the I.A. function perceived by managers seems related to the size and age of the internal audit structures, that appear more effective in carrying out their tasks. Only half of the sample is perceived as value generating by the respective managers. On the other hand, C.A.E. declare that division and top managers are only partially aware of their role inside the internal controls system; this is a worrying fact, since the corporate governance code entitles them as “the first and second line of defense” against risks.

To help solve some of the criticalities above listed, possible interventions will now be proposed.

The confusion around the role of the internal auditor has to be tackled. Positive steps appear to be done with horizontal turnover made by the I.A. functions examined, and much effort can be done with the spread of the audit charter inside companies. Also, communication skills have to be developed by internal auditors not to appear as “watchdogs” but as an important body able to issue strategic advices.

For what concerns the techniques adopted by the auditors, quantitative methodologies have to be empowered both in audit field work and in risk assessment. Those techniques, once mastered, provide more reliable data in comparison with personal estimations, and can accelerate some audit tests.

Finally, from the Italian Space Agency case presented in Chapter 6 it has been shown that for the national scenario internal audit can be useful also in state-owned organizations and that auditors with experience in private companies can enhance the tasks carried out by a controlling body inside those organizations. This is a possible example of how the profession could evolve in the future.

Appendix A

Internal Audit Survey

Question 1: For how long does the I.A. function exist?

- Less than 5 years
- From 6 to 10 years
- For more than 10 years

Question 2: Which events led to the introduction of the function?

- Acquisition by a group adopting I.A.
- Internal events
- Growth of the company
- Listing process in a Stock Exchange

Question 3: At which level is the function positioned in the group?

- Holding
- Sub holding
- Subsidiary

Question 4: How many people are employed? Part-time workers worth 0.5.

Question 5: How many people outside the company are employed on average in the I.A. function?

Any part-time workers will be counted as 0.5. Consultants are not considered.

Question 6: Which are the professional profiles most represented in the function?

- Studies in business or economics
- Experiences in external auditing
- Experiences or studies in antifraud
- Experiences or studies in risk calculation
- Accounting

Question 7: On average, for how long do the components remain in the I.A. function?

- Less than 3 years
- From 3 to 5 years
- From 5 to 8 years
- More than 8 years

Question 8: What is the annual budget dedicated to the function?

Question 9: From which body of the corporate governance framework does the I.A. function depends?

- Board of directors
- C.E.O.
- Chairman of the board of directors
- Director responsible for the internal control and risk management system
- Audit committee
- Board of statutory auditors

Question 10: With which bodies is there a closer and more frequent contact?

Assign a score from 1 (almost no contacts) to 4 (frequent contacts).

- Board of directors
- C.E.O.
- Chairman of the board of directors
- Director responsible for the internal control and risk management system
- Audit committee
- Board of statutory auditors
- Supervisory body ex D.Lgs 231 of 2001

Question 11: Which of these mechanisms are most important for the transmission of information within the internal control system?

Assign a score from 1 to 4.

- Periodic meeting with the bodies composing it
- Approval of the audit plan
- Cross memberships

Question 12: Who nominates the responsible of the I.A. function in the company?

- Board of directors (with the favorable opinion of the other members of the system of internal controls)

- C.E.O.
- Board of statutory auditors

Question 13: Who are the addressees of the periodic reports?

- Board of directors
- C.E.O.
- Director responsible for the internal control and risk management system
- Board of statutory auditors
- Supervisory body ex D. 7
- Lgs 231 of 2001
- Control and risk committee

Question 14: Does the C.A.E. think that the reports are considered by the recipients?

- Yes, all reports
- Yes, but only superficially
- No
- I don't know

Question 15: Does the C.A.E. take part to the controls and risks committee's meetings?

- Always
- More than 50% of the meetings
- Less than 50% of the meetings
- Never

Question 16: What kind of relation does exist between the C.A.E. and the supervisory body ex D. Lgs 231 of 2001?

- Member or chairman of the supervisory body
- The I.A. function is the supervisory body
- Always participates to the meetings
- Sometimes participates to the meetings
- Never participates to the meetings

Question 17: What kind of relation does exist between the C.A.E. and the person responsible for the preparation of the corporate financial documents ex L. 262 of 2005?

- Strict relation during the creation of the financial statements
- Advisory role required sometimes
- No relation

Question 18: How often is the C.A.E. consulted in the definition of the business strategies?

- Often consulted
- Sometimes consulted
- Never consulted

Question 19: How often do all the main business processes receive an audit?

- Less than 2 years
- From 3 to 5 years
- More than 5 years

Question 20: How much importance does the following elements did receive during the preparation of the last audit plan?

Assign a score from 1 to 4.

- Compliance
- Efficiency and effectiveness of the operations
- Maintaining the value
- Reliability of the financial statements
- Reaching company's strategic objectives

Question 21: The audit plan is:

- Written by the C.A.E. and approved by the board of directors
- Imposed to the C.A.E. from other bodies
- Discussed with other bodies

Question 22: How much do the following characteristics of a process weight into the creation of the audit plan?

Assign a score from 1 to 4.

- Risk
- Materiality
- Dimension of the process

Question 23: In average, how much does an audit lasts?

- One week
- Two weeks
- Three weeks
- A month
- More than a month

Question 24: How much time-absorbing are the following activities during and audit?

Assign a score from 1 to 4.

- Risk assessment and preliminary survey
- Engagement programme
- Field work
- Reporting and issuance of advices
- Follow-up
- Archiving activities

Question 25: Before starting an audit, does the C.A.E. always control the design of the controls over a process?

- Yes
- No
- Only for some processes

Question 26: During field work, how often does the C.A.E. uses the following audit techniques?

Assign a score from 1 to 4.

- Physical calculation of objects
- Interviews to those conducting the controls daily
- Surveys
- Reperforming control procedures
- Sending confirmation letters to third parties
- Reconciliations
- Recalculation
- Trend analysis
- Documentation sampling

- Regressions and statistical models

Question 27: In percentage, during an audit, how often is a walkthrough conducted?

Question 28: During antifraud test, how often are the following techniques used?

Assign a score from 1 to 4.

- Controlling unusual transactions
- Controlling end-period transactions
- Controlling related-parties transactions
- Controlling managers' estimations

Question 29: Through which documents are audit results archived?

It is possible to mark more than one answer.

- Photocopies
- Confirmation letters
- Surveys' results
- Photographs
- Results of statistics tests
- Working papers
- No documents are archived

Question 30: In percentage, how many audits do receive a follow-up?

Question 31: How does the C.A.E. considers relations with the management?

- Management respects and trust the I.A. function
- Minor contrasts are present with managers
- The I.A. function is often critiqued and hampered by managers

Question 32: Which are the major sources of resistance from the management?

It is possible to mark more than one answer.

- Misunderstanding of the I.A. function's role
- Misunderstanding of the way of working of the I.A. function
- Management considers inadequate the members of the I.A. function

Question 33: In the opinion of the C.A.E., management consider the I.A. function:

- As value generating
- Merely necessary for compliance reasons

Question 34: How much importance does the following elements of the internal control system have in the company?

Assign a score from 1 to 4.

- Control environment
- Risk assessment
- Control procedures
- I.T. reliability
- Monitoring

Question 35: Managers are aware of their role inside the internal control system?

- Totally aware
- Aware but not totally
- Only limitedly aware
- Not aware

Question 36: Does it exist a shared method to prioritize risks for the whole company?

- Yes, every function uses a shared method
- No, but similar methods are used
- No, every function prioritize risk following a different method

Question 37: During the risk assessment phase, which typologies of instruments are used?

- Mostly quantitative instruments (statistics, mathematical models, indexes etc.)
- Mostly qualitative instruments (estimations)
- Only quantitative instruments
- Only qualitative instruments

Question 38: How is calculated materiality by the I.A: function?

- Through a mathematical method based on financial ratios
- Through the auditor's judgement (estimation)
- Generally, it is not calculated

Bibliography

ABRIANI, N., CALVOSA, L., FERRI, G., et al., 2012. *Diritto delle società. Manuale breve*. 5° edition. Milano: Giuffrè Editore.

ADAMS, M., B., 1994. Agency theory and the internal audit. *Managerial auditing journal*, 9 (8), pages 8-12.

AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS, 2002. *Statement on Auditing Standards (SAS) No. 99: Consideration of Fraud in a Financial Statement Audit*. Durham: American Institute of Certified Public Accountants.

ALLEGRI, M., edited by, 2011. *Risk reporting e sistemi di controllo interno. Un'analisi comparata tra Italia e regno Unito*. Milano: Franco Angeli.

ALVARO, S., CICCAGLIONI, P., SICILIANO, G., 2013. *L'autodisciplina in materia di corporate governance. Un'analisi dell'esperienza italiana*. Roma, CONSOB.

ARENA, M., ARNABOLDI, M., AZZONE, G., 2006. Internal audit in Italian organizations. A multiple case study. *Managerial auditing journal*, 21 (3), pages 275-292.

AURELI, S., CIAMBOTTI, M., SALVATORI, F., 2011. *Strategic Risk Management nelle aziende di servizi pubblici locali italiane: prospettive teoriche ed empiriche* [online] Available at:

https://www.researchgate.net/publication/281206348_strategic_risk_management_nelle_aziende_di_servizi_pubblici_locali_italiane_prospettive_teoriche_ed_empiriche.

[Access date:12/01/2017].

BIANCHI, N., 2010. Corporate governance con più coordinamento. *Il Sole 24 ore* [online]. Available at:

http://www.ilsole24ore.com/art/norme-e-tributi/2010-11-08/corporate-governance-coordinamento-064059_PRN.shtml.

[Access date: 02/01/2017].

CALIFORNIA PUBLIC EMPLOYEES' RETIREMENT SYSTEM, 2015. *CalPERS Global governance principles*. Sacramento: CalPERS.

CHEFFINS, B. R., 2012. *The History of Corporate Governance*. ECGI Working Paper Series in Law, Working Paper N° 184/2012. Available at:

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1975404

[Access date: 07/12/2016].

COMITATO PER LA CORPORATE GOVERNANCE DELLE SOCIETÀ QUOTATE, 1999. *Codice di autodisciplina (Codice Preda)*. Milano: Borsa Italiana S.p.A.

COMMITTEE ON THE FINANCIAL ASPECTS OF CORPORATE GOVERNANCE, 1992. *Report of the committee on the financial aspects of corporate governance (Cadbury Report)*. London: Gee.

CONGRESSIONAL RESEARCH SERVICE, No date. *S. 2567 (96th): protection of shareholders rights act of 1980*. Available at:

<https://www.govtrack.us/congress/bills/96/s2567/summary#>

[Access date: 08/12/2016].

CONSIGLIO NAZIONALE DELLE RICERCHE, 2013. *1° Programma di audit – presentazione dei risultati*. Rome: Consiglio nazionale delle ricerche.

COOMBES, P., WONG, S. C.Y., 2004. Why Codes of Governance Work. *The McKinsey Quarterly* [online], N° 2. Available at:

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=897422

[Access date: 20/12/2016].

CORPORATE GOVERNANCE COMMITTEE, 2015. *Corporate governance code*. Milano: Comitato per la corporate governance.

CORBELLA, S., PECCHIARI, N., edited by, 1999. *Internal auditing. Aspetti di struttura e di processo: i risultati di una ricerca empirica*. Milano: EGEA.

COMMITTEE OF SPONSORING ORGANISATIONS OF THE TREADWAY COMMISSION, 2004. *Enterprise risk management-integrated framework*. Jersey City: Committee of sponsoring organisations of the Threadway commission.

COMMITTEE OF SPONSORING ORGANISATIONS OF THE TREADWAY COMMISSION, 2013. *Internal Control - Integrated Framework. Executive summary*. Jersey City: Committee of sponsoring organisations of the Threadway commission.

DEMARTINI, P., GRAZIANI, P., MONNI, S., edited by, 2012. *Performance. Sistemi di controllo. Made in Italy*. Roma: RomaTrE-Press. Page 42.

DE MOLLI, V., VISANI, M., 2015. I vantaggi del modello monistico. *Il sole 24 ore* [online]. Available at:

<http://www.ilsole24ore.com/art/commenti-e-idee/2015-08-05/i-vantaggi-modello-monistico-063758.shtml?uuid=ACKmu8c>

[Access date: 11/12/16].

DIPIETRO, B., 2015. The Morning Risk Report: Companies Adopting Updated COSO Framework. *The wall street journal* [online]. Available at:

<http://blogs.wsj.com/riskandcompliance/2015/04/29/the-morning-risk-report-companies-adopting-updated-coso-framework-newsletter-draft/>

[Access date: 13/01/2017].

DRAGO, C., et al., 2011. *Directorship networks and company value in Italy (1998-2007)*. CESIFO Working Paper N° 3322.

EILIFSEN ET AL, 2010. *Auditing and assurance services. 2nd ed*. London: McGrawHill.

ENRIQUES, L., VOLPIN, P., 2007. Corporate governance reforms in continental Europe. *Journal of Economic Perspectives*. Volume 21, Number 1-Winter 2007-, pages 117-140.

FINANCIAL REPORTING COUNCIL, 2016. *The UK corporate governance code*. London: The financial reporting council limited, page 10.

FINANCIAL REPORTING COUNCIL, 2005. *Internal control: Revised guidance for directors on the combined code*. London: The financial reporting council limited.

HOYT, R. E., LIEBENBERG, A. P., 2011. The value of enterprise risk management. *The journal of risk and insurance*. 78 (4), pages 795-822.

INTERNATIONAL AUDITING AND ASSURANCE STANDARD BOARD, 2015. *The Handbook of international quality control, auditing, review, other assurance and related services pronouncements*. New York: IFAC.

LA PORTA, R., et al., 1999. Investor protection and corporate governance. *Journal of financial Economics*, 58 (2000), pages 3-27.

LA MANNO, F., 2012. *Il sistema di controllo interno e di gestione dei rischi nel nuovo Codice di Autodisciplina* [online]. Milan: Borsa Italiana. Available at: www.aitiaweb.it/utenti/download/anonimi/avv._lamanno.pdf [Access date: 31/12/16].

LO DICO, A., 2008. *L'attività di internal audit in un gruppo internazionale. il caso Guess*. Master Thesis, Università degli Stufi di Firenze.

LIEBENBERG, A., P., HOYT, R. E., 2003. The determinants of enterprise risk management: evidence from the appointment of chief risk officers. *Risk Management and Insurance Review*, 6 (1), pages 37-52.

McSHANE, M. K., NAIR, A., RUSTANBEKOV E., 2011. Does Enterprise Risk Management Increase Firm Value? *Journal of Accounting, Auditing & Finance*, 26 (4), pages 641–658.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, 1999. *OECD Principles of corporate governance*. Paris: Meeting of the Council at Ministerial Level.

PICKETT K.H.S., 2010. *The internal audit handbook*. 3° edition. Chippenham: Wiley.

PAAPE, L., SPEKLÉ, R. F., 2011. *The adoption and design of enterprise risk management practices: an empirical study*. European accounting review, forthcoming. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1658200

[Access date: 13/01/2017].

POWER, M., 2009. The risk management of nothing. *Accounting, organizations and society*. 34 (2009), pages 849-855.

PROTIVITI, 2014. *Internal auditing around the world. Building on experience to shape the future auditor*. Protiviti inc.

PRICEWATERHOUSECOOPERS, 2016. *Internal auditing nelle società quotate. Approfondimenti sull'informativa fornita al mercato*. PricewaterhouseCoopers Advisory SpA.

PRICEWATERHOUSECOOPERS, 2014. *Internal control environment. Key considerations and developments*. PricewaterhouseCoopers Business Solutions SA.

RAMAMOORTI, S. 2003. *Internal auditing: history, evolution and prospects*. Alamonte Springs: The institute of internal auditors research foundation.

RENN, O., 1998. Three decades of risk research: accomplishments and new challenges. *Journal of risk research*, 1 (1), pages 49-71.

ROBERTS, J., MCNULTY, T., STILES, P., 2015. Beyond agency conceptions of the work of the non-executive director: creating accountability in the boardroom. *British journal of management*, volume 16, issue s1, pages 5-26.

ROMANO, R., 2004. *The Sarbanes-Oxley Act and the Making of Quack Corporate Governance*. Yale Law School, Nberm ECGI: Working Paper No. 04-032. Available at: <http://ssrn.com/abstract=596101>

[Access date: 12/12/2016].

SECURITIES AND EXCHANGE COMMISSION, 1976. *Report on questionable and illegal corporate payments and practices*. Washington, U.S. Government printing office.

SEGATTO, C., 2013. *La gestione dei rischi aziendali e l'Enterprise Risk Management. Il caso italiano*. Master Thesis, Ca' Foscari University of Venice.

SELIM, G., WOODWARD, S., ALLEGRINI, M., 2009. Auditing and consulting practice: a comparison between UK/Ireland and Italy. *International journal of Auditing*, 13. Pages 9-25.

THE INSTITUTE OF CHARTERED ACCOUNTANTS IN ENGLAND AND WALES, 1999. *Internal control: guidance for directors on the combined code (Turnbull report)*. London: The institute of chartered accountants in England and Wales.

THE INSTITUTE OF INTERNAL AUDITORS, 2016. *International standards for the professional practice of internal auditing (standards)*. Altamonte springs, Florida: The Institute of Internal Auditors Inc.

THE INSTITUTE OF INTERNAL AUDITORS, 2013. *International professional practices framework (IPPF)*. Altamonte springs, Florida: The Institute of Internal Auditors Inc.

THE INSTITUTE OF INTERNAL AUDITORS, 2004. *Internal auditing's role in sections 302 and 404 of the U.S. Sarbanes-Oxley Act of 2002*. Altamonte springs, Florida: The Institute of Internal Auditors Inc.

TETTAMANZI, P., 2000. *Controllo interno, revisione interna e corporate governance in Italia e nel Regno Unito. Un'indagine empirica*. Liuc papersn.80, Serie Economica Aziendale. Available at: <https://ebiblio.istat.it/SebinaOpac/.do?idDoc=0031700#4>
[Access date: 19/01/2017].

WAYNE, L. 1994. *Have shareholder activists lost their edge?* The New York Times, 30 January, pages 3-7.

WILBURN, A., J., 1984 *Practical statistical sampling for auditors*. New York: Marcel Dekker.

WRIGHT, M., SIEGEL, D.S., KEASEY, K, edited by, 2013. *The Oxford Handbook of Corporate Governance*. Oxford: Oxford University Press.

ZATTONI, A., 2015. *Corporate Governance*. Milano: EGEA.

