ANRA

Associazione Nazionale dei Risk Manager
e Responsabili Assicurazioni Aziendali

Risk Management Standards and ISO 31000

Adopting consistent processes within a general structure of reference so as to contribute to ensuring that risk is effectively managed, with efficiency and in a consistent manner throughout the organisation.

Risk Management Standards and ISO 31000

ANRA Position Paper

9 November 2011

In cooperation and with the support of Strategica Group

Paolo Rubini

President ANRA

In a macroeconomic setting in which the vulnerability of enterprises is increasing, Risk Management is increasingly to the forefront of the attention of many directors and senior managers, who ask questions concerning the manner of identifying, measuring and dealing with corporate risks in from a systematic standpoint.

ANRA responds to this need by publishing a document describing the process of Risk Management, as defined in ISO 31000 Guide Lines: these are the outcome of international best practices, starting life in Australia and England, received by FERMA the European Federation of Risk Management Associations and finally transferred into a general model that represents the new frontier of the profession.

Enrico Guarnerio

President Technical Scientific Committee ANRA

Acting in a globalised economic setting has led to an awareness of the need to face up to situations that bring about management of risks that are ever more detailed and complex.

The requirement for ever greater transparency, the wish to manage risk in a scientifically structured manner by adopting shared and internationally recognised methodologies, can only be to the advantage of the development of the professionalism and the significance of the role of the Risk Manager.

Index

1. Aims of the Position Paper

Organisations in general, whether small/medium enterprises or large corporate groups, today find themselves more than in the past having to face up to themes connected with the likelihood of events that make the achieving of their objectives uncertain.

The effect of this uncertainty in achieving corporate objectives is defined as "risk"[1].

We all know that carrying on any type of economic activity leads to taking risks. However today, thanks to the growth in management culture and discipline, studies and research carried out on the risk management, the suggestions of sector associations and effects of orders from lawmakers aimed at ensuring even greater transparency in market briefing, we are witnessing an ever greater interest in the advantages offered by Risk Management activities.

ANRA, in 1972, started life with the purpose of actually disseminating the culture of corporate risk management.

The publication of ISO 31000 Standards by the Technical Committee ISO/TMB "*Risk Management*" has led ANRA to creating a study Group of professionals from the sector and risk managers of important companies with the purpose of analysing and studying its contents in depth.

This document has as its main aim the divulging of ISO 31000 standards, selected by ANRA as a model of reference for carrying on the activity of Risk Management, and providing the reader with a summary description and a key for reading its main contents.

The Position Paper concludes with a description of the possible interdependencies of the players intervening in activities of Risk Management.

1. The term risk a has been translated into Italian language as "possibilities of an event and its consequences on objectives" UNI/ISO 11230:2007 Risk management - Dictionary

2. Reference context

The function of Risk Management, for the very reason of being introduced within the area of corporate governance, follows the discipline regulating the system of corporate organisation[2].

As comes to light when reading the provisions of law issued in the last decade, the corporate organisational system that is coming to the forefront aims to ensure corporate management that is healthy and prudent and pursues financial and equity stability by containing risks, and propriety and transparency of behaviour of parties involved in the production of goods and/or provision of services. The provisions governing the Risk Management functions fall under the principles that underlie the general discipline in matters of corporate governance.

The request made of organisations to arrange for there to be solid tools of company governance has led community and Italian lawmakers to introduce into legal systems, although initially by specific sectors, of detailed obligations in respect of preventing certain risks, starting from protection of the physical integrity of the "worker" party, going as far as a new conception of the activity of prevention of risk required of the "enterprise" party, and necessary too as a element that is subject to *disclosure* for the general protections of the "market" party[3].

Connected with the theme of risk management there is also the configuring of the responsibilities of corporate management towards the market (stakeholders, oversight authorities. Liabilities attributable within the broader function attributed to economic imitative which, according to our Lawmakers "*cannot be carried on in conflict with social utility or in manner such as to do injury to security, liberty and human dignity*" (Art. 41 of the Constitution).

Referring also to this principle contained in our fundamental Charter, in recent years a number of sectors, especially the banking, insurance and financial sectors, have been the

2. Publication in 1999 of the Code of Self-discipline, the so called Preda Code, by the Committee for *Corporate Governance* of Listed Companies set up by Borsa Italiana S.p.A., represents a fundamental term of reference for defining criteria of *Corporate Governance*. The code, which has been updated a number of times, contains recommendations for guidance such as to make up the model of "best practices" for organising and proper functioning of Italian listed companies.

3. See also directive no. 2003/51/CE relating to annual accounts and consolidated accounts of a number of types of company, banks and other financial institutions and insurance companies; directive 2014/109/CE on the harmonising of duties of transparency concerning information in respect of issuers whose equity securities are admitted to negotiation in a regulated market; directive 2012/76/EU in the matter of equity requirements for portfolios in negotiation and securitising and review of compensation policies by oversight bodies. By these orders the obligation of disclosure was, among others, introduced in respect of the main risks of companies whose equity securities are admitted to negotiation in a regulated market and operating within a Member State and the series of companies, even unlisted, included in consolidation.

subject of a detailed regulations aimed at creating functions of oversight and control in internal and external to the enterprise, as well as new forms of liability for the purpose of ensuring greater stability of the enterprise to the advantage of market reliability.

In a perspective of Corporate Governance therefore, the theme assessment of risks is entwined with that deriving and implementing the system of internal control to ensure corporate efficiency and effectiveness, safeguarding corporate property and compliance with laws and regulations.
The function of risk management is furthermore consistent and attributable to the provisions of unavoidable Legislative Decree no. 231/2001 in the matter of administrative liability of legal persons[4].

As we all know, a number of "delicate" sectors have already been bound to foresee the function of Risk Management within the organisations concerned. In particular, the banking and insurance sectors and healthcare, in addition to listed companies, in abidance by the duties deriving from the discipline involving the drawing up of financial statements.

Similarly, listed companies are the recipients of similar duties assigned, in abidance by provisions that have as their subject matter the discipline in respect of drawing up financial statements.

However, even for many other sectors we can see that there is a growing number of rules that, more or loss directly, incorporate the need for the presence within the corporate organisation of an activity of Risk Management.

See for example the consolidation act on safety at work and the Environmental Code protecting health and safety of society[5].

In the sector of large scale distribution and consumer and user services, the Consumer Code includes among the duties of the manufacturer and distributer, protecting the purchaser, adopting measures that are proportionate based on the characteristics of the product supplied, and that include "*opportune initiatives to avoid risks occurring*" tied to a broad concept of defectiveness of the product (Art. 104, paragraph 3 of the Consumer Code).

Expectations concerning the preparing of a profile or a protocol aimed at managing risk in the company have had full recognitions in the decisions taken by courts of justice,

4. Legislative Decree no. 231/2001 *Discipline in respect of the administrative liability of legal persons, companies and associations even without legal personality.* The order "invites" any type of company to adopt adequate organisational models for preventing the occurrence of crimes actually listed in the decree, through arranging adequate and efficient administrative organisation and company accounting. Legislative Decree 231/2001 does not contain prescriptive rules, but adopting a corporate organisational model arranged in an "adequate" manner grants a judge legitimacy in the event of the crimes foreseen in the order occurring, and an exemption from liability of the company.

5. See: Legislative Decree 81/2008 and subsequent amendments, Consolidation Act in the matter of protection of health and safety in work places and Legislative Decree no. 152 dated 3 April 2006, Environmental Code.

which have ruled in the matter of failure to adopt adequate organisational models in the terms of Legislative Decree 231/01 and safety measures to protect consumers (e.g. risk of product recall).

2.1. Listed companies

The lawmaker has issued detailed provisions directed towards listed companies aimed at taking advantage of adequate analyses and management of corporate risks.

The Consolidation Act on Finance which governs the sector foresees, among other things, the duty for delegated administrative bodies and senior managers who deal with drawing up corporate accounting documents, to attest by means of a specific report attached to the financial statements for the accounting period, and the consolidated one, to having arranged adequate administrative and accounting procedures directed towards forming the financial statements and all other notices of a financial character.

The management report includes a reliable analysis of trends and the result of management as well as the situation of the issuer and the companies included in consolidation, together with a description of the "main risks and uncertainties they are exposed to"[6].

It should be borne in mind moreover that the provisions of the Civil Code in the matter of financial statements intended for publications relating to the regime of waivers foreseen under art. 2423 of the Civil Code, sets forth that "*If the information required by specific provisions of the law are not sufficient for giving a truthful and proper representation, complementary information necessary for the purpose must be given*". It should be noted that the waiver is not to be understood as being a discretion but rather a duty foreseen for the purpose of safeguarding the clause in respect of truthful and proper representation. Whereas Art. 2423-bis of the Civil Code "Principles for drawing up financial statements" imposes in drawing up financial statements, abidance by the following principles: assessment of the headings in accordance with prudence and from a perspective of a going concern; [...] 4) and which takes into account risks and losses concerning the accounting period, even if becoming known after this closes; [...].

Consider too, concerning art. 19, paragraph 1, letter b) of Legislative Decree 39/2010, that in dictating rules in the matter of legal auditing of annual accounts and consolidated accounts, imposes upon bodies of public interest that the internal control committee and accounting audit "oversee the effectiveness of the system of internal control, internal auditing, if applicable, and risk management".

The general interest and the importance that lawmakers attribute to the Risk Management function is further demonstrated by the fact that the Ministry of the Economy and Finance requires specific skills in the matter of "risk management and internal control" in respect of those who wish to take the examination of professional fitness to earn the

6. See art. 154 *bis letter* e) of Legislative Decree no. 58/1998 as modified in 2005 by law no. 262 to protect savings.

qualification of accounting auditor (art. 4 of Legislative Decree no. 39/2010)[7]. This latter provision is contained also in directive 2004/109/CE so called "Transparency Directive".

2.2. The banking sector

In respect of matters concerning the banking sector, consider the joint regulation by the Bank of Italy and Consob, issued in 2007, wherein the system of enterprise risk management is indicated for Banks, SIMs, and financial intermediaries as being made up of: "*the strategies, policies, processes and mechanisms concerning the identification, assuming, management, oversight and mitigation of risks to which the intermediary is or may be exposed (among which being credit, market, operating reputational and strategic risks) and to determine and control the tolerated levels of risk*" (Joint Regulations of the Bank of Italy and Consob, Art. 2 Definitions).

Harmonised regulations in the matter of compensation policies and practices and directed towards banks and investment enterprises – introduced by European directive no. 2010/76/EU in harmony with the internationally agreed and approved principles of the Financial Stability Board, impose upon the Board of Directors of credit bodies the involvement of functions of internal control (Internal Audit; Risk Management and Compliance) and human resources in defining compensation policies[8]. According to directive no. 2010/76/UE, compensation regimes must be "adequate", i.e. set so as to be able to avoid "the assumption of excessive and imprudent risks" which in the past have unfortunately led in a number of States to the arising of systemic risks in addition to the bankruptcy of numerous credit institutions.

2.3. The insurance sector

In the insurance sector too, as for the banking sector, the new system of "risk based" oversight of solvency has been introduced[9].

In particular, we have directive no 2009/138/CE, so-called Solvency II. The directive defines a new solvency regime granting, as compared to the current regime, greater relevance to the quality of risk management and the solidity of internal controls. In this regard, the Solvency II directive sets forth that insurance companies must conduct within their system of risk management, an internal assessment of risk and solvency (so-called ORSA, *Own Risk and Solvency Assessment*). This assessment concerns the global solvency requirement, account being taken of the specific risk, limits of risk tolerance approved by the Board of Directors and the operating strategy of the enterprise.

7. Legislative Decree no. 39/2010, Implementation of directive 2006/437CE relating to legal audits of annual accounts and consolidated accounts, modifications of directives 78/660/CEE and 83/349/CEE and abrogation of directive 84/253/CEE.

8. Directive 2010/76/UE implements the order of the Bank of Italy dated 30 March 2011. The directive sets out agreed principles and standards in the international area and sits within the wider listing of measures aimed at ensuring the stability and good functioning of the banking and financial systems in respond to the crisis. To ensure applications and property and homogeneous interpreting of it within the European Union the directive was accompanied by Guide Lines of the CEBS (European Banking Authority as from 1st January 2011).

9. Directive 2009/138/CE in the matter of access to and carrying on insurance and reinsurance businesses, so-called Solvency II. In this sector, as in the banking sector, a series of European directives has been emanated which, in effect, have extended the principles contained in the Basle II rules to the insurance sector.

As long ago as 2008, the national oversight authority for the sector, ISVAP, had introduced by regulations no. 20/2008 the duty applying to insurance companies of creating internally a Risk Management function appropriate for the nature, size and complexity of its activity.

This function responds to the administrative body and its organisational placement must be such as not to depend on operating functions; in abidance by art. 21 of these regulations, the function of Risk Management:

a) takes part in defining the methodologies for measuring risks;
b) takes part in defining operating limits assigned to operating structures and defines the procedures for timely verification of these limits;
c) validates the flows of information necessary for ensuring timely control of exposure to risks and immediate detection of anomalies found in operations;
d) prepares reporting forms of operating structures towards the administrative body, senior management and heads of operating structures concerning trends in risks and breach of the operating limits set;
e) verifies the consistency of models of measurements of risks with the operations performed by the enterprise;
f) takes part in effecting stress tests.

On the other hand publication of ISVAP regulations no. 39/2011 in respect of compensation policies of insurance companies is recent and which, in line with international leanings, must be consistent with healthy and prudent management of risk and in line with strategic objectives [...] (art. 4 regulations 39/2011)[10]. The regulations assign to the Board of Directors the duty of involving the internal control functions (Internal Audit, Risk Management and Compliance) and Human Resources in defining compensation policies together with creating mechanism of incentive that take into account, "*where appropriate, also the objectives of a non economic kind, such as compliance and efficiency in the management of client services*" (art. 12, paragraph 2, letters a and b)[11].

Also the regulatory provisions of the oversight Authority of the insurance sector aim to implement an efficient system of management involving insurance companies directly via the requirement to proceed to self-assessment of the capacity of current compensation systems to meet regulatory provisions[12].

10. SVAP Regulations no. 39/2011 art. 4 General Principles: *Enterprises are to adopt compensation polices consistent with health and prudent management of risk and in line with strategic objectives, profitability and balance of the enterprise in the long term. 2 Enterprises are to avoid compensation polices based exclusively or prevalently on short term results such as to create incentives to excessive exposure to risk.*

11. Insurance companies are bound to adopt compensation policies that measure the performance of directors on the basis of indicators that take into account risks associated and correlated charges, within a non brief temporal horizon [...] and that create mechanism of incentives that take into account "*where appropriate also of the objectives of a non economic kind, such as compliance and efficiency in management of client services*" (ISVAP Regulations no. 39/2011 art. 12)

12. With effect from 1st January 2011 the new oversight Authorities of the European financial sectors at a macro and micro prudential levels are operational; the EIOPA superintends the insurance area.

2.4. The healthcare sector

The sector that more than any other has already for years leant towards defining the functions of Risk Management is surely the healthcare sector. The importance of identifying and managing risks and so-called sentinel events for the purposes of protecting health of citizens has seemed to be of basic importance in offering healthcare services.

The main orders in the matter of risk management in healthcare have been drawn up by the Ministry of Health. Already in 2004 the document titled "*Risk management in healthcare. The problem of errors*" had been drawn up. In 2006 the Glossary in the matter of patient safety and clinical risk management was created. The subsequent year there was the "*Protocol for sentinel events in addition to the Recommendations for preventing acts of violence against healthcare operators*".

In 2009 there following the Recommendation for the prevention of adverse events consequent upon malfunctioning of medical devices /electrometrical equipment.

The relevance of the role of Risk Manager, today present within healthcare structures, is fundamental for defining the protocols for risk management for each operating unit. Abidance by protocols has now become a consolidated pattern of behaviour in performing professional activity by operators of the sector.

A number of regions have had follow the introduction of the Risk Management function periodic mapping of the risks of all Hospital companies, Local Healthcare companies and Foundations with public investment operating under the aegis of the Regional Healthcare Service[13].

13. See document of the Lombardy region; General Healthcare Management, Mapping of risk in the Healthcare System, 2011

3. Risk Management Standards

Companies need to understand the aggregate level of risks implicit in their processes and their activities. This implies recognising and giving priority to the most significant risks, identifying criticalities, recognising the weaknesses of controls and achieving implementation of an effective Risk Management process.

The design and implementing of risk management plans and defining their reference structures require taking into consideration the various demands of specific organisations, their objectives, their setting, their structure, their operations, their processing functions, their plans, products and services and the specific practices adopted.

In recent years there has been constant growth in the need to manage risk ever more effectively and rigorously, integrated into overall governance, into the strategy, planning and management of process of reporting, into the policies, values and culture of the company.

This requirement has led to a search for and adopting of processes that are increasingly structured, so as to contribute to ensuring that risk is managed effectively and in a manner that is consistent with the organisation overall.

Standards of reference

Formalising a Risk Management process its content, the players involved and the manner of assessing risk management strategies has involved numerous associations in implementing studies of documents useful for evidencing the characteristics of the Risk Management model. Building up Guide Lines for process standards has allowed companies to adopt the model best fitted to their needs, abiding by national and international rules that individual organisations must follow.

The best known standards are:

- AIRMIC, ALARM, IRM 2002. Standards drawn up by the largest Risk Management organisations of the United Kingdom, taken up later also by the European Federation of Risk Management Associations – FERMA;
- Co.So II, 2004. Published by the *Committees of Sponsoring Organizations of the Treadway Commissions* (a private US body that deals with internal controls and Corporate Governance), the document describes the principles, components and most relevant concepts in corporate risk management, with special attention given to the roles and tasks of the various functions from a Corporate Governance standpoint[14].

14. The Co.So. Report (*Committees of Sponsoring Organisations of the Treadway Commission*) is one of the most used models in the world for implementing plans and programmes of Risk Management. It is used for the management of integrated risks (ERM: Enterprise Risk Management) and offers a rich section of alternative techniques to support application of the model.

- AS/NZS 4360:2004 First standard drawn up in Australia/New Zealand that provides generic guidelines for the Risk Management process.
- AZ/NZS – ISO 31000:2009. Development of the previous Australian standard, developed in European ISO Standard and adopted both in Europe and later in Australia/New Zealand.
- ISO Guide 73:2009 – Vocabulary, 2009. A guide that brings together the meanings of the technical terminology related to the process of Risk Management in English.
- ISO 31000, 2009. The document titled "Risk Management. Principles and guidelines" contains the guide lines for applying art. 41 second paragraph, letter b of directive 2006/43 in respect of annual and consolidated accounts (implemented in Italy by Legislative Decree no. 39/2010).
- ISO 31010:2009. The document titles "Risk Management Techniques" which supports the ISO 31000 standard providing indications on specific techniques of risk assessment.
- UNI ISO 11230:2007. Risk Management. Vocabulary in Italian language.
- UNI ISO 31000, 2010 The document titled "Risk Management Principles and guide lines" is a translation into Italian of ISO 31000 guide lines.

The advantages of applying a standard

Adoption of an internationally recognised Risk Management standard allows, in general, an increase in the degree of awareness of the need to manage risks, an improvement in the effectiveness and efficiency of risk management and the system of controls, renders the decision making process more reliable, improving the quality of risks and augmenting the confidence and trust of stakeholders internal and external to the enterprise.

4. The ISO 31000 Standard

The ISO 31000 Standard was drawn up in 2009 by the ISO/TMB "*Risk Management*" Technical Committee[15].

The ISO 31000 standard provides the principles and guide lines for management of any form of risk in a systematic, transparent and credible manner and within any field of application and setting.

The ISO 31000 standard promotes harmonising of the processes of risk management but without forgetting the need for specific consideration connected with each company, and providing a common approach to support rules that concern specific sectors and/or risks, but without replacing these rules.

Te peculiarity of the ISO 31000 standard arises from its applicability to **any type of enterprise** (irrespective of the specific sector concerned) in connection with its various **areas of activity** (including strategies, operating processes, development of projects), and **any type of risk** it is exposed to (whatever may be the nature or the consequences, positive or negative that is may generate).

The ISO 31000 standard sets forth a number of principles that must be abided by in order to render risk management effective and recommends that organisations develop, implement and continuously improve a reference structure whose purpose is to integrate the process of risk managements within that of overall governance of the enterprise. Applying the ISO 31000 standard allows definition and uniformity of processes of risk management, replicating them within the organisation.

The ISO 31000 standard intends to meet the needs of a vast range of stakeholders, among who are, in particular: heads of development of risk management policies within the organisation, those who must ensure that risk is effectively managed and those who need to assess the effectiveness of the organisations in managing risk.

The structure of ISO 31000 standard is based on the relationship between **Principles** that must be abided by in order to manage risk effectively, the **Structure of reference** in which the risk management is implemented[16], and the **Risk Management Process** [17].

In the chapters that follow the individual components of the standard are illustrated.

15. The same ISO 31000 standard was subsequently brought in, in the Italian language, under the concern of the UNI Technical Committee "Safety of society and the citizen" and was definitively approved on 25 November 2010.

16. Figure 1 shown in the chapters that follow

17. Figure 1 shown in the chapters that follow

5. The principles

The ISO 31000 standard indicates a series of principles which should inspire an organisation for achieving effective risk management.

According to the principles provided by ISO 31000, risk management:

a) creates and protects value;
b) forms an integral part of all organisational processes;
c) forms part of decision making processes;
d) deals explicitly with uncertainty;
e) is systematic, structured and timely;
f) is based on the best information available;
g) is "made to measure";
h) takes into account human and cultural factors;
i) is transparent and inclusive;
j) is dibasic, iterative and reactive to change
k) favours continuous improvement in the organisation.

Risk management effected with a systematic, timely and structured approach:

- contributes in a demonstrable manner to achieving objectives and improving performance;
- is not an independent activity, separate from the main activities and processes of the organisation;
- aids in making aware choices, determining the scale of priorities of actions and distinguishing between alternative lines of action;
- contributes to the efficiency and to results that are consistent, comparable and reliable
- favours the appropriate and timely involvement of stakeholders and, in particular, those responsible for decisions, at all levels of the organisation.

Organisations should develop and implement strategies for improving risk management systems together with all the other aspects of their organisation.

6. The structure of reference

All organisations should aim at an appropriate level of performance of its structure of reference for risk management in line with the criticality of the decisions to be taken.

Account being taken of the fact that risks are considered in terms of "*effect of uncertainty on objectives*", their management is considered central for management processes of the organisations and essential for achieving the objectives themselves.

Success of risk management depends therefore on the effectiveness of the management structure of reference, which provides the foundations and the arrangements for integrating risk management into the entire organisations, at all levels.

The structure of reference has the task of ensuring that the information relating to risk obtained from the management process, are brought, in abidance by the communication and reporting programmes, to the decisional bodies pertinent in the matter.

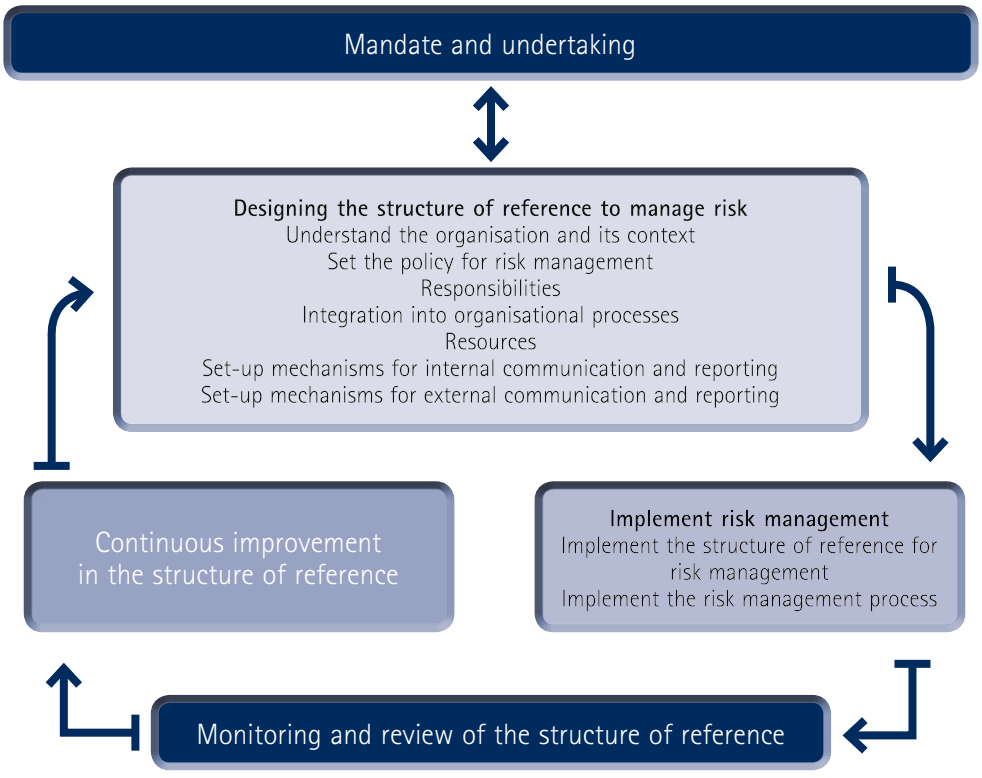

Figure 1:
Relations between the components of the structure of reference to manage risk. Source: UNI ISO 31000

The management structure of reference must be structured for the purpose of supporting risk management activity through applying the risk management process at various corporate levels, integrating risk management within the overall management system, and achieving adaptation of the components of the structure of reference to specific corporate needs.

The company and constant commitments by management of the organisation, together with rigorous strategic planning, is an indispensible factor for effective risk management and its lasting application.

The objectives of risk management must obviously be consistent with the objectives and strategies of the organisation and with its culture. Prior even to commencing the design phase and implementing the reference structure for managing risk, management must assess and understand the context of the organisation, both internally and externally, as the peculiarities of the various settings may influence the design of the structure itself significantly.

Communications and sharing of pertinent information by the reference structure within the company lead to greater responsibility being taken at all levels of the organisation, whereas it will be the task of management to notify to stakeholders of the benefits of risk management activities undertaken, given the delicate nature of the information.

However, positive effects of risk management will be achieved only if each organisation has the ability to seek out and recognise within itself the persons who, given their experience, are able to build the structure of reference best fitted to carrying out this task.

The various degrees of responsibility at the various levels within the organisation must be assigned, checking periodically upon how appropriate they are and ensuring that the structure has resources that are adequate so as to be able to perform the activity properly. It may be found fitting in this regard to assign specific objectives and determine clear indicators of performance for the purpose of favouring continuing improvement in risk management.

7. The Risk Management process according to the ISO 31000 standard

The process of risk management can be presented as a listing of coordinated activities and by a cyclic sequence.

The ISO 31000 standard has conceived the Risk Management process foreseeing a number of main phases – identification, analysis, evaluation and treatment of risk – evidencing, too, the that prior defining of the context, monitoring and communications are at all times elements that are basic for implementing Risk Management activities correctly (cf. Figure 2).

It is important to point out that the process of risk management must not only form an integral part of strategy and management of the enterprise, but also be a management tool that is incorporated into the culture and practice of the organisation.

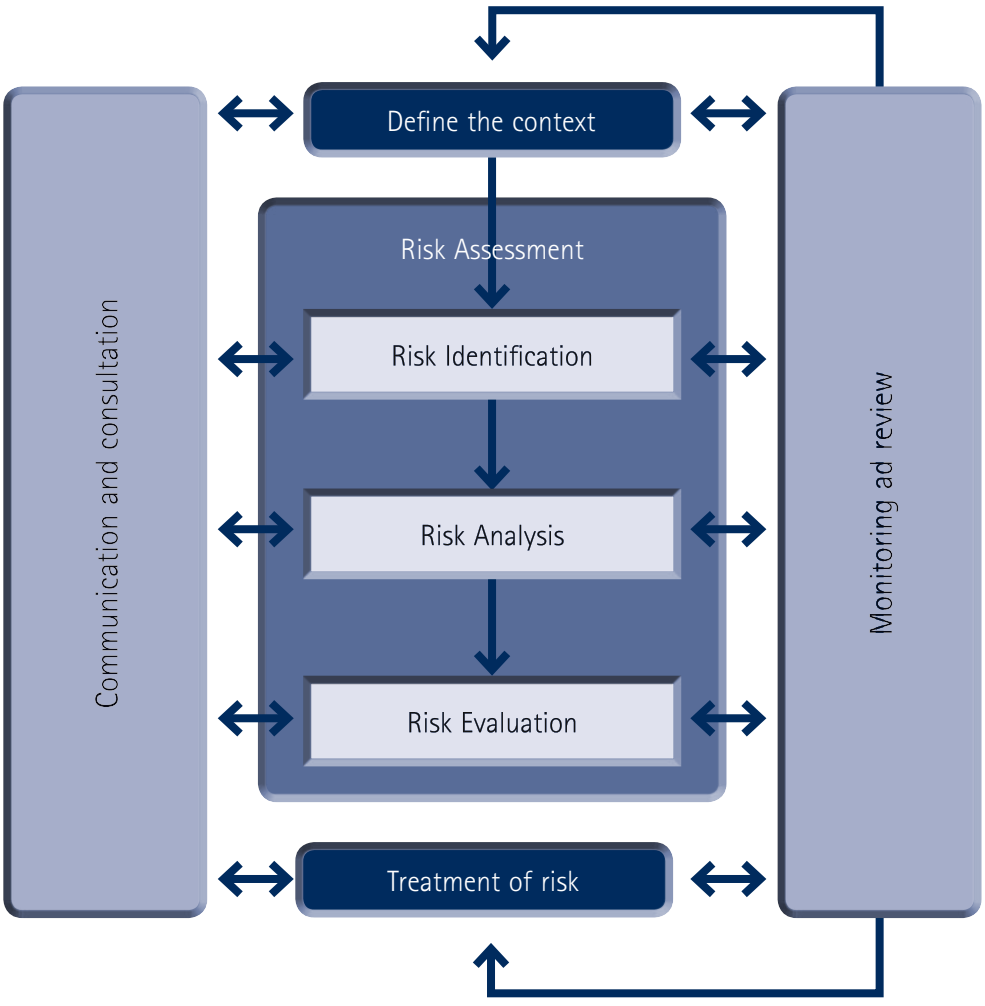

Figure: 2:
Process of risk management.
Source:
UNI ISO 31000

In the representation of the process according to the ISO 31000 standard, communication and consultation and monitoring and review should be implemented at each phase of the process and not only as final element, as they are essential for the process to run properly.

The typical phases of risk management are improved thanks to clear and shared procedures, in addition to through continuing interdependency between players and functions.

7.1. Communication and consultation

Plans for communication and consultation concern the risk in itself, its causes, consequences and measures taken to deal with it. Plans of communications must be set up in such a way that stakeholders can assess the circumstances and take specific decisions.

Activities of communication and consultation, while taking into account issues of personal integrity and confidentiality, ought to take place during all the stages of the risk management process, as they are indispensable for effectiveness and the outcome of the entire process.

The best approach for maximising the effects of consultation is "team working": management must define the setting in an appropriate manner, ensure that risks are adequately identified and that the needs of stakeholders are included and considered. It must moreover be able to create specific analyses bringing together various areas of concern, taking different standpoints into consideration appropriately in actually defining the risk criteria and risks evaluation.

Comprehensibility and accuracy in drawing up the information is also found to be of fundamental importance, both for communicating a plan for dealing with risk adequately and for intensifying and having stakeholders understand the actions necessary in change management that is taking place for developing the Risk Management process.

7.2. Definition of the context

An important feature of the ISO 31000 standard concerns the introduction of "defining the context", as being a preliminary activity to the process of risk management.

Risk management is an ongoing process that supports the development and implementation of the strategies of an organisation and which must face up to all the risks associated with any activity of the organisation methodically. This implies awareness of critical factors of success, the threats and the opportunities tied to achieving the objectives.

Defining the context allows the objectives of the organisation, the environment in which it pursues the objectives, the stakeholders concerned and the diverse nature of the risks to be grasped, which are elements that all contribute to detecting and assessing the nature and the complexity of risks.

In order to carry out a proper analysis of risks, organisations must first of all define the context in which the company deals in connection with its objectives, identifying the external and internal parameters applying, and selecting the criteria of risk that will be considered in implementing the process.

The external context

Comprehending the **external context** represented by the environment where the company seeks to pursue its objectives is important for ensuring that the ends and the concerns of external stakeholders are adequately and properly considered in developing criteria of risk.

The external context is made up of the deciding factors and fundamental trends that have a bearing on the objectives of the organisation such as the social, political, financial, technological, economic, natural and competitive environment and relations with external stakeholders.

The internal context

The **internal context** is represented by the internal environment where the organisation seeks to achieve its objectives and features anything, within the organisation itself that may have a bearing on the way the organisation intends to manage risk.

The risk management process cannot be separated from an understanding of the internal context, as it must of necessity integrate with the culture, the processes, the structure, the strategy and the objectives of the organisation. This implies awareness and a complete understanding of issues of governance, roles and responsibilities assigned within the organisation, as well as the relationship with the processes, resources available, features of relationships with stakeholders, systems, flows of information, decision making processes, regulations, guide lines and models adopted by the company.

The context of the risk management process

Risk management should be undertaken on the basis of the objectives and areas of application within the organisation of the company, this also for the purpose of allocating resources necessary for achieving the expected results.

Defining the context of the risk management process should help ensure that the adopted approach to risk management is appropriate to the circumstances, the organisation and the risks that have a bearing on achieving the objectives sought. This implies, by way of example, defining the responsibilities, the activities, the objectives, the functions, projects, risk assessment methods, the criteria for assessing performance and the effectiveness of risk management.

Define the risk criteria

At the context definition stage, the organisation should moreover define the criteria to be used in assessing the significance of the risk.

These criteria should reflect the values, objectives and resources of the organisation, be consistent with the risk management policy and then be reviewed continually.

The main criteria to be considered concern: identifying the risk sources, defining the manner of measurements of risk levels, defining the risk level of risk that the organisation is wiling to bear (appetite for risk and/or risk tolerance), the correlation between risks, the time horizon and the methods of measuring the causes and consequences of events.

7.3. Risk Assessment

The risk assessment stage overall is taken up by the activities of identifying, analysing and evaluating risks.

7.3.1. Identification

The risk identification stage consists of selecting and evidencing the risk sources, the events, causes and potential effects of occurrences that may impact upon critical factors of success, and on achieving the objectives of the organisation.

The objective of this stage is to generate a complete listing of risks, avoiding leaving out events that otherwise would not be considered in subsequent analyses.
Identification must include an examination of the indirect effects of special consequences including the cascade or cumulative effects, and consider a broad range of consequences significant or otherwise, even if the source or cause of the risk might not be apparent.

The company must apply tools and techniques for identification suited to its objectives and capabilities and the risks it has to face; at this stage it is important for the information to be pertinent and up-to-date and derive also from prior knowledge and experience.

In identifying risks, persons with appropriate knowledge should be involved.

7.3.2. Risk Analysis

Risk analysis implies developing an awareness of risks and features an assessment of the positive or negative consequences (impact) and the likelihood (probability) deriving from the occurrence of individual risks at the identification stage.

The results of the analysis, and the manner in which they are expressed, provide the data and the elements necessary for proceeding to the decision making process, featuring subsequent phases evaluation and treatment of risk. Reports should highlight any critical factors such as differences of opinion, availability and quality of information and limits in modelling.

In order to know the enterprise risk profile in-depth analysis of its components is necessary. The analysis can be undertaken in various degrees of detail on the basis of the risk, the purpose of the analysis and the data and resources available, and should consider the level of effectiveness and efficiency of existing control systems as well as the consistency of the assessments with the risk criteria defined during the examination of the context.

The analysis may be carried out by means of modelling in qualitative, semi-quantitative or quantitative form of the data available, which may in their turn be represented by events recorded or extracted from experimental studies. An element with special relevance that must be considered is the interdependency between different risks and related sources.

The results of the analysis may also be expressed in terms of tangible and intangible impacts and, if the case, may express more than one numeric value or one descriptive term.

The combination of impact and probability, the manner in which the information available is expressed, the purpose for which the existing data are used, the interdependency between different risks and relative sources, all reflect the level and the type of risk of the organisation.

7.3.3. Risk Evaluation

The risk evaluation stage considers the criteria of risk set forth during the examination of the context and the results of the risk analysis, and aims to define which risks need treatment and the related priorities for implementation.

Taking into account the risk appetite of the organisation and the risk criteria established, decisions may be limited to keeping existing controls active without proceeding to a further risk treatment stage or, alternatively, proceeding to a further analysis stage.

7.4. Risk Treatment

Following the decision taken at the evaluation stage, the Risk Management process foresees moving on to the risk treatment stage, featuring assessment of the options most fitting for modifying the profile of risk and implementing action plans.

Risk treatment is marked by a cyclical process which foresees assessment of the risk treatment options, assessment of the effectiveness of the options chosen and consideration of the tolerability or otherwise of residual levels of risk downstream of treatment.

Risk treatment normally foresees implementing different possible solutions such as: elimination of the sources of risk (also through giving up performing the activity underlying it), assuming the risk so as to pursue an opportunity, modification of probabilities of occurrence and/or impact of the consequences, sharing the risk with other parties (transfer), retention of the risk in an aware manner.

The choice of the best suited treatment option implies obtaining the best relationship between costs of implementing and benefits deriving from this, taking into consideration any requirements of a mandatory kind.

Risk treatment requires the involvement of various stakeholders, among whom the level of risk may be perceived in different ways.

Risk treatment must be based on a structured plan depending on the priorities for intervention and must be monitored so as to verify the effectiveness of the measures adopted.

The plan of risk treatment must be fully integrated within the organisation and adequately documented, indicating: the parties involved both at the approval and at the implementation stage, the criteria for the choice of option of treatment, the expectations in terms of outcome, action plans, requirements relating to resources, parameters of performance measurement and requirements for reporting and scheduling intervention.

Downstream of the process of treatment implemented, the residual risk should be reviewed involving persons responsible for decision making and other stakeholders, so as to be subjected, if opportune, to further treatment.

7.5. Monitoring and review

The risk management process foresees planning of monitoring activities and a scheduled review, which require regular verification of all issues making it up.

Monitoring and review activities serve to ensure the effectiveness and the efficiency of controls, ensure a flow of information needed for analysing the risk, analysing the events, detecting changes in the context (internal, external and related to defining the risk criteria) that may have a bearing on the level of risk, and possibly requires revisions be made to treatments and priorities.

The results of monitoring must be recorded and referred to in the most fitting manner and provide the elements needed for reviewing the reference structure for risk management.

In addition to monitoring the effectiveness of existing controls, the global efficiency of activities and the setting up of further controls, monitoring must ascertain the cost-benefit relationship of existing controls.

Finally, monitoring and measurement include an assessment of the dissemination of the culture of risk, performance and preparation of the organisation, the awareness of the reference structure, and an assessment of the extent to which the tasks of risk management are aligned with other corporate activities and the routine monitoring of performance indicators.

8. Roles and players in the Risk Management process

Defining the roles and duties that the various parties must fulfil within Corporate Governance has been established thanks also to the determination of Systems of Internal Control (SCI): the parties and the functions contributing to the management of the enterprise in a manner that is healthy, proper and consistent with corporate objectives and Risk Management have been carefully and jointly identified by international organisations whose objective was to delineate clearly the key points of the system of enterprise governance from the standpoint of efficiency and adherence to regulatory principles, without overlapping of activities.

Three lines of defence, or levels of control, were then defined and aim to identify the responsibilities, roles and tasks of the various functions involved in the control and management of corporate risks.

Risk management is a discipline that forms part of these levels of control.

On the basis of the nature and the size of the organisation, Risk Management may be run by a consultant performing implantation of analysis and process of Risk Management for a limited time and for individual categories of risk, or the function may be created within the company, aimed at developing plans of Risk Management fit to last over time. The various responsibilities concerning the management of risks that must be shown in documents of corporate policy are broad and extensive. It is important in this regard to avoid possible overlapping roles, assigning a function that is clear and well defined to the Risk Manager who must work alongside other corporate heads.

In order to disseminate the culture of risk and set in motion plans of risk management, the Risk Manager, together with their team, must have transverse skills, going from the insurance area to management of enterprise, from compliance to awareness of the goods sector in which the company operates. They cannot replace the risk owner or become owner of risks that do not concern them, so as not to breach the principle of accountability. However, in order coordinate all the players taking part in the process of risk management effectively, they must know the installations, production cycles, margins of contribution, features of products to be sold and services to be provided; they must know and know how to implement methods for designing specific plans for management of risk, considering not only the activities and the processes that the company has in being, but also carrying out careful analysis of the context in which it operates and the prospects for development of the organisation.

8.1. The figure of the Risk Manager

The aim of the Risk Manager is to promote, at all levels, the activity of risk management, with growth in the responsibilities taken on by all staff in respect of specific policies of watching over risk.

The Risk Manager has a strong leaning towards motivating persons, planning and control, and the capacity to translate the needs of the Board of Directors into strategic actions aimed at mitigating risks with adverse effects and taking advantage of exploiting opportunities arising from a series of risks.

The Board of Directors has the general responsibility for determining the strategic course of the organisation and is propensity for risk, creating the context and the structure for management risk, including the most significant risks and managing the company in times of crisis.

In this context, the Risk Manager will work alongside those responsible for all corporate functions and will support them in their decisions on risks specific to the function and play a role of coordination of decisions on risks that are transverse over a number of functions. They must know how to create the conditions for setting in motion mechanisms that are adequate for obtaining continuous improvement in performance, maintain a dialogue with function managers so that implementation of recommendations for improving the level of risk is ensured, and ensure that new risks and circumstances are identified and properly reported.

Additionally the Risk Manager must be able to have the process of Risk Management understood, accepted and implemented so as to reach achievement of reports that also contain reporting of events that could have been configured as adverse/loss making events and that evidence the existence of a potential situation or risk (so-called sentinel events).

The direct responsibilities of the Risk Manager – as owner of the process of Risk Management – are on the other hand based on developing and updating a policy of risk, continuous updating concerning the specialist activities of the sector, coordinating of the risk management function and its activities, compiling informative reports concerning preponderant risks, the development of emergency and recovery plans and support given to inquiries. The Risk Manger must be able to control the process of Risk Management within the global activities of the company, receive guarantees in respect of management of risk and make reports on efficiency and effectiveness of internal controls.

In particular, the Risk Manager must support Management in identifying risks and, in so far as they are responsible for the functioning of the process, must provide those responsible for function or division the tools necessary for identifying and assessing individual corporate risks. As the activity to be performed must be continuous within each organisation, its decisions must be supported by an adequate system of briefing gathering all the information on risks and allowing a simpler stage of consolidation of results to take place.

After the drawing up of the plan of Risk Management, the Risk Manger must have approval from corporate senior management for implementing the programmes in respect of individual activities to be carried out. Together with the highest levels of the organisation the strategic, tactical and operational objectives that are indispensible for obtaining economic-financial results from the processes set in motion by the company must be identified. The Risk Manager must assign specific responsibilities at each level of the organisation and notify relevant information, procedures and specific objectives so as to disseminate the culture of risk and obtain feedback concerning the essential processes for enterprise activity.

8.2. Interdependence with other main administrative and control figures

The configurations of interdependencies and interrelations between the Risk Manager, or the function to which it refers, and other corporate figures, is different, based on the corporate dimensions, vision and approach. In the boarder vision of Corporate Governance the relations between functions are determined by systems of internal control that have the objective of ensuring adequacy of the manners of control as compared to the risks to be watched over.

The "*Guidance for Boards and Audit Committees*", a document published on 21 September 2010 and drawn up jointly by FERMA (European Federation of Risk Management Associations) and by ECIIA (Confederation of Institutes of Internal Auditing), defined three levels of defence with the aim of ensuring adequacy of the manners of control as compared to the risks to be watched over.

Operational management forms the first line of defence, being the series of persons who have ownership, responsibility and accountability in assessing, controlling and mitigating risks and keeping internal controls effective.

The second line of defence includes the Risk Management function. This function defines as the framework of risk management, facilities and controls implementing of effective practices in risk management by operational managers, assists the risk owner in defining the exposure to risk and reports the information connection with risk within the organisation. In addition to the Risk Management functions, as part of the second line of defence, a number of organisations have foreseen a distinct function of Compliance to monitor risks of non-fulfilment, i.e. risks of non compliance with laws and regulations, even internal ones. In this capacity, the Compliance function reports directly to senior management.

Other specific control functions may be directed towards health and safety of staff, the supply chain or issues of environmental protection and/or quality.

The third line of defence is formed by the internal audit function. This function, via a risk based approach, provides assurance to the Board of the organisation and Senior Management in respect of how the company assesses and manages its risks, including a description of the manner via which the first and second line of defence operate.
The activity of control performed by Internal Audit contributes to identifying, managing

and keeping under control, possible adverse events so as to provide reasonable certainty concerning the achieving of the objectives of the organisation.

All the activities performed within the three levels of control, are directed towards Senior Management and the Board of Directors who have full powers of decision making concerning the final management of risks identified.

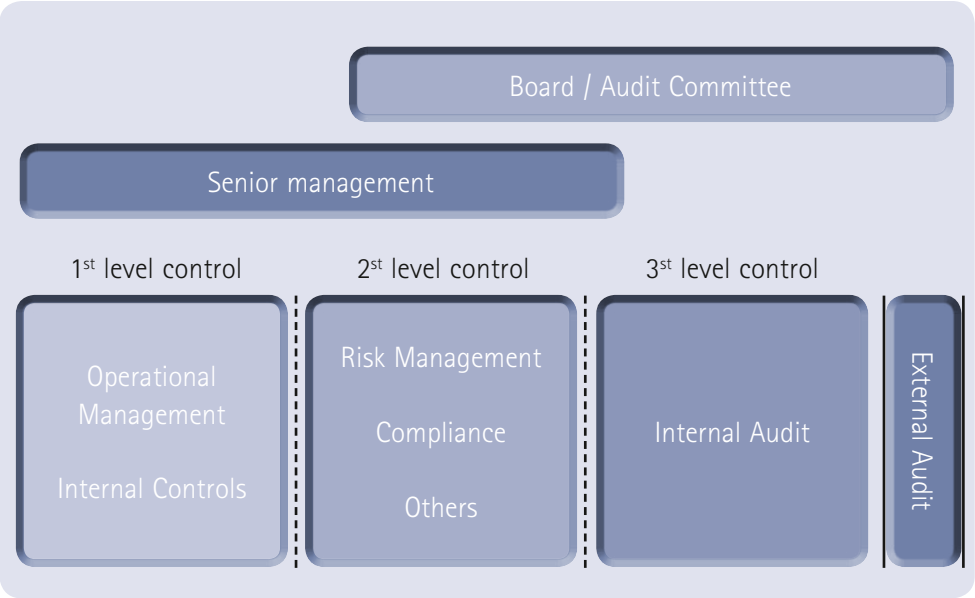

Figure 3:
The three levels of Internal Control Systems.
Source: FERMA/ECIIA

The Board of Directors supervises and issues the guide lines to management defining the "risk appetite", is aware of the most significant risks of the organisation and has as final objective verification as to whether or not middle management is responding in an appropriate manner to the request of the board and other cooperate needs.

Defining its expectations in terms of integrity and ethical values, the Board of Directors provides general objectives to management and sets forth the indications concerning allocation of resources. One of the main tasks in the area of risk management is to supervise the process of Risk Management acquiring knowledge of the extent to which management has activated an effective process of corporate risk management. The Board of Directors must define the level of risk that is acceptable for the company, but also examine the actual risk.

Internal Audit must on the other hand carry out a function of assurance on the effectiveness of the processes implemented. The objective is to provide assurance of adequate management of the main corporate of risks and proper and effective implementation of the process within the corporate system.

The complementary nature of the figure of Risk Manager and Internal Auditor derives from the wish of both to support management in managing risk.

ANRA

ANRA is the association that since 1972 has brought together Risk and Insurance Managers.

ANRA counts the Risk Managers of the largest Italian companies among its members.

ANRA plays a central role in creating and developing a risk management culture in Italy and is a mandatory interlocutor on issues relating to Risk Management.

ANRA is the institutional contact for disseminating international best practices coordinating with FERMA (the Federation of European Risk Management Associations) and IFRIMA (the International Federation of Risk and Insurance Management Associations), of which it is a Founder Member.

The following contributed to preparing this document.

Paolo Rubini
President of ANRA
Head of Risk Management Telecom Italia S.p.A.

Enrico Guarnerio
President of ANRA Technical Scientific Committee
President and Managing Director, Strategica Group S.r.l.

Marco Terzago
Director ANRA
Group Risk Engineering Manager -
Risk/insurance Manager South East Europe SKF Industrie S.p.A.

Roberto Bosco
Director ANRA
Corporate Risk Manager, Mediaset S.p.A.

Alessandro De Felice
Director ANRA
Group Chief Risk Officer
Prysmian S.p.A.

Domenico Fumai
Risk Management Telecom Italia S.p.A.

Rita Cricitto Ph.D.
Visiting Lecturer L. Bocconi University Milan
Head of Scientific Division studies and research Strategica Group S.r.l.

In cooperation and with the support of

Strategica Group

PARTNER IN RISK MANAGEMENT

www.strategicagroup.com