Liability of corporations in Italy and risk prevention: toward a cloud-governance system

Barbara Gaudenzi*

Department of Business Administration,
University of Verona (Italy),
Via dell'Artigliere n. 19, 37129, Verona, Italy
E-mail: barbara.gaudenzi@univr.it
*Corresponding author

Gianluigi Lucietto

Risk Consulting Network,
Via Eleonora Duse n. 12, 37124, Verona, Italy
E-mail: lucietto@riskconsulting.it

Pietro Domenichini

Istituto di Studi sulla Responsabilità Amministrativa degli Enti,
Via Nizza n. 5, 37121, Verona, Italy
E-mail: pietro.domenichini@istituto-isr.eu

Abstract: This research describes the Italian regulation on liability of corporations (Italian Legislative Decree 231 issued in 2001) and the consequent requirements in terms of risk management and corporate governance. Starting with an analysis of the literature on the relationships among governance, risk management and compliance, the paper investigates the new challenges emerging from this legislative scenario. Moreover, the paper describes the critical phases towards the implementation of a managerial risk management process that helps managers to monitor all the responsibilities imposed by the Decree. Finally, the paper analyses when and how cloud-based solutions can support companies in managing critical risks, and particularly those risks that are formally mentioned by the Italian regulation on liability of corporations.

Keywords: governance; liability; risk assessment; risk prevention; cloud computing; organisational models; auditing technology.

Reference to this paper should be made as follows: Gaudenzi, B., Lucietto, G. and Domenichini, P. (2013) 'Liability of corporations in Italy and risk prevention: toward a cloud-governance system', *Int. J. Auditing Technology*, Vol. 1, Nos. 3/4, pp.277–293.

Biographical notes: Barbara Gaudenzi is an Associate Professor of Risk Management of the University of Verona, Italy. She is Director of the Post Graduated Course in Risk Management and Director of LogiMaster (Master in Supply Chain Management) of the University of Verona (Italy). Her research interests focus on supply chain risk management and she has published refereed articles in international journals and Italian journals. She coordinates and is involved in research projects with companies and public organisations.

Gianluigi Lucietto is an Independent Risk Management Consultant for a selected number of manufacturing companies operating in Italy. He is a Contract Professor of Risk Management of the University of Verona and in the Post Graduated Course in Risk Management (riskmaster.it). He is one of Founder of Academic Risk Management Association (arimas.it), and is Associate in Risk Management at the Insurance Institute of America (theinstitutes.org).

Pietro Domenichini is Criminal Lawyer and President of many 'Organismi di Vigilanza', boards of professional advisory. He founded in 2005 the 'Istituto di Studi sulla Responsabilità Amministrativa degli Enti', an independent no profit research and education association targeting corporate responsibility and provides solutions for risk management and corporate responsibility prevention.

1 Introduction

In the current environmental context, the roles of the governance and its boundaries change: the push from globalisation leads organisations to face with many stakeholders, in international markets and networks. In addition, the competition is increasing the time of reaction, innovation (time) should be combined with the optimisation of the cost/quality ratio of products/services and risks are increasing.

The recent evolutions in the legislative and socio-economic scenario have set up new conditions for governance systems and regulations.

In the last ten years in USA with the well-known Sarbanes-Oxley Act (2002), and a few years before also in Europe, legislators and supervisory bodies have imposed clearer and stringent business liability regimes, and raised the level of 'criminal penalties'. It is not a casualty that this trend started after the Enron and Worldcom scandals (2002).

Besides moral arguments associated with fairness and the rejection of the unique focus on profit maximisation, corporate governance should focus on the value creation for stakeholders in a long term perspective, improving controls and looking beyond contractual liabilities.

This new legislative and environmental scenario could represent a positive challenge for organisations. These must incorporate the meaning of new regulations and stakeholders expectations in their decision making processes and systems, making – at the same time – their processes more resilient. Otherwise, there could be a risk to underestimate the significance of these rules and to mismanage emerging risks.

In this paper, we describe the recent legislative scenario in Italy for legal responsibility imposed by the Decree 231 issued in the year 2001, that introduces a new kind of responsibility for the entities (without regarding if they are public o private organisation, profit or not), which is named penal and administrative responsibility for entities. This new regulation represents a significant challenge for improving an integrated risk management (IRM) process and a governance system in all the organisations.

In the paper a review of the literature reveals three emerging trends. First, value creation, risk and compliance are closely related (Pirson and Turnbull, 2011), and the link is represented by an effective governance system. Second, risk management plays a

strategic role for the company's success, particularly when an IRM allows for evaluating and managing all the 'enterprise wide' risks (*ERM Framework*, 2004). Third, web technology and cloud systems are becoming increasingly sophisticated, and can allow information sharing and decision making.

Given this backdrop, the paper investigates the opportunity to use cloud-based solutions for integrating risk management and governance systems, in order to respond proactively to emergent requirements imposed by regulations.

In detail, the specific objectives of this paper are:

a to analyse the Italian situation in the field of liability of corporation, and the consequent requirements in terms of corporate governance

b to understand the relationships among governance, risk management and compliance

c to investigate when and how cloud-based solutions can support companies in managing critical risks, and particularly those risks that are formally mentioned by the Italian regulation on liability of corporations.

Hence, we will propose a framework for implementing a cloud-governance model, which can support managers in monitoring critical risks and responding to legislative requirements. The Decree 231 imposes that managers adopt all the actions in order to prevent crimes, with respect to the principles of the 'good governance' based on risk management approaches.

The model is established as an 'identification, measurement, treatment, implementation and audit (IMTIA) process', which takes foundation from the best risk management standards and good practices nowadays available.

In describing this model, the paper aims at contributing to the limited literature on empirical examples of risk assessment practices (Borghesi and Gaudenzi, 2012).

2 Background

Companies are facing an increasingly competitive scenario. The need to simultaneously manage diverse and at times opposing strategic objectives leads organisations to take greater levels of risk. Therefore, the conditions of riskiness are linked to both the environmental context and the strategic and managerial choices made by organisations' managers.

2.1 Value creation, governance and compliance

Nowadays, competitive models focus on the capability of the company to maximise the stable creation of value for all the stakeholders.

Hence, all the value-added processes, planning and control systems and organisational structures should be strictly related to the objective of maximising the value creation.

Managing with a view to create value begins with the strategy and ends with the financial results: managers are responsible for creating the link between strategy and results. The mission of the value creation gives rise to strategies, organisational models and new management systems that, considered as a whole, found their theoretical

foundation in the value-based management (VBM) theories (Copeland et al., 1996; Elgharbawy and Abdel-Kader, 2013).

In the VBM perspective the three basic elements of an organisation's long-term competitiveness are:

1 the value creation is the primary scope of business processes

2 the decision-making process should be oriented toward the capability to create value

3 organisational structures and resource allocation should facilitate the value creation.

The top management should therefore establish the organisational system, coordinate the key sub-systems, plan and guide development actions. It means that the governance system is responsible for both ensuring the economic objective of maximising value creation and complying with a 'social task': that is the balance of interests and the social legitimisation with and from various public reference models (Premkumar et al., 2005).

The Organization for Economic Co-operation and Development (OECD) has provided a definition of the contents of corporate governance, which are closely related to the areas of the above cited legislative applications. The pillars of the corporate governance systems are in particular the board of directors' liability, the commitment to a effective corporate governance, the role of stakeholders (commitment to disclosure and transparency) and the fair treatment of shareholders (Borghesi and Gaudenzi, 2012).

Therefore, corporate governance extends beyond the area of relationships with shareholders only, based on the agency theory or shareholder value theory (Fama et al., 1996), and affects all the stakeholders in their capacity as parties responsible for the social legitimisation of the company (Pirson and Turnbull, 2011; Rahim, 2012). The significant focus on social legitimisation resulting from many stakeholders represents one of the reasons why today reputation is so important and reputational risk is addressed as a strategic priority for many companies (Christopher and Gaudenzi, 2009).

Stakeholders have more access to information and demand greater transparency and responsibility from businesses (Thomas et al., 2009). For these reasons, the 'global' governance (Brawn and Caylor, 2004; Jones et al., 1997) should embrace in its competency different dimensions, such as the internal dimension (employees); the networking dimension (co-makers and partners); the integration dimension (global market); the transparency dimension (shareholders and finance); and the corporate ethics dimension (government and media).

Hence, the role of 'compliance' has increased significantly in importance, in all the countries and in Italy (Bartolomucci, 2004; Daccò, 2004). This role includes compliance with regulations and the proper disclosure of corporate choices to all the stakeholders' categories.

With this scope corporate governance systems should introduce voluntary rules (codes of conducts and self-regulations, resulting from the internal control system) and a systematic approach to monitoring the entire compliance system (*ERM Framework*, 2004).

The final purpose is to ensure an integrated 'compliance' with binding regulations, and also with effective decision-making processes, and with efficient operations.

In this regard, we note that where there is a need for so-called 'global' governance systems, for example for organisations operating on international markets, the risk management models become more complex.

2.2 Integrated risk management

The risk management process is particularly relevant because it has the objective to protect the organisation from unfavourable events, in order to maximise its value creation capacity.

An IRM approach allows for the coordination of strategic processes, through the effective and efficient management of those risks that are typical of key business processes (Dickinson, 2004).

A common understanding of risk and risk management should therefore be applied consistently throughout the firm. In the past risk management aimed at managing 'insurable risks', that are risks linked particularly to incidents that could damage physical and financial resources. Starting in the 1980s though, authors began to stress the importance of an IRM, which allows for the integration of strategic, financial, and operational management (Emblemsvåg, 2010). Today, three widely applied approaches to IRM are the ISO Guide 31000 (ISO 31000, 2009), the enterprise risk management (ERM) framework (*ERM Framework*, 2004) and the risk management standard proposed by AIRMIC et al. (2010).

Hence, the major benefits of IRM are the evaluation and management of those risks, which can threaten a company's competitiveness. Moreover, IRM can support decision-making processes, focusing on well-established value creation priorities. In addition, an effective risk management approach aims at optimising the cost of capital and the cost of risk (Borghesi and Gaudenzi, 2012). From these perspectives, the ERM framework (*ERM Framework*, 2004) has gained increased consideration over the last ten years. The term 'enterprise' is intended to stress the holistic nature of the risk management process. ERM, in particular, aims at responding to the legislative requirements, such as Sarbanes-Oxley act for companies listed in the USA, also aligning to the principles of the 'good governance'. The ERM framework comprehends controls and consultation tools for the purpose of meeting both external and internal compliance requirements.

Nevertheless, the concrete application of these risk management approaches is only partially developed in the practice. Bandyopadhyay et al. (1999) evidenced that IRM often cannot really support holistic decision-making processes and that IT technologies represent a potential area of development.

2.3 Cloud computing

Cloud computing refers to both the applications delivered as services over the internet and the systems in the data centres that provide those services (Armbrust et al., 2010; Mola and Carugati, 2012).

Besides many applications of cloud computing in different business areas and sectors, there are some recent studies highlighting the potential benefits of these solutions for risk management, governance and compliance (Farrel, 2010).

Considering in particular that regulatory innovations impose a direct involvement of internal and external stakeholders in decision-making processes, cloud-based systems may facilitate information sharing and control procedures.

Cloud services and systems can be structured on the basis of three models, related to different technological solutions and integration's levels: infrastructure-as-a-service (IaaS) (storage, processing, and network services), platform-as-a-service (PaaS)

(development, testing, deployment, hosting, and maintenance services), and software-as-a-service (SaaS) (web application usage services) (Mell and Grance, 2009; Gold et al., 2004).

Looking at the usability of cloud systems, significant applications are reported in the field of risk and security management. Gens (2008) and Farrel (2010) reported the emergent role of cloud computing technologies in order to face the multi-form threats for organisations that are related to security. Kaufman (2009) and Gatewood (2009) noted the importance to integrate the identification of key risks, the audit controls and the organisational procedures.

While cloud systems can effectively support the decision-making process and information sharing, these also require an effective management and controls for their inherent risks (ISACA, 2009). These IT systems can contribute to the creation of significant risks, because companies transfer data to third parties for storage, processing or support. Protecting intellectual property and information are therefore key challenges. For this reason, developing detailed cloud breakdown scenarios and performing recovery run-throughs is essential. Large part of the literature describes how to develop a risk-mitigation strategy before moving into the cloud environment (Gold, 2012). Moreover, it should be noted that a robust decision-making process should be established before implementing a cloud computing system (Ferrari et al., 2012). In this way, IT systems can facilitate the information sharing, also producing relevant cost advantages, as reported by Benlian and Hess (2011). In addition, an appropriate selection of the service providers is essential, in order to evaluate costs and performance of different tools. In this sense, Fan et al. (2009) proposed an interesting analysis of key drivers for rating service providers, like for example user implementation costs, operation efficiency, and quality improvement over time.

Without a well-established managerial procedure, cloud computing cannot support decision-making and can generate indirect and hidden costs (Walterbusch et al., 2013). Taking these suggestions, cloud systems can be considered as effective tools for making the risk management process more integrated and usable by decision makers. Before developing such a IT system, the risk management process should be verified for its robustness (Gens, 2008).

3 Liability of corporations and compliance: focus on the Italian evolution

The recent evolutions in the legislative and socio-economic scenario have set up new conditions for governance systems. In various countries, legislators, international authorities and supervisory bodies have made regulations ever more stringent.

The promulgation of laws and rules, that impose on companies stringent obligations related to governance principles and procedures, has stimulated investments aimed at ensuring a better control and protecting themselves from the risk of non-compliance. We wish to briefly mention some of the more effective initiatives, like the Sarbanes-Oxley Act (USA, 2002), the Combined Code on Corporate Governance (USA, 2003, new version in 2006), the Turnbull Guidance (UK, 1999) and subsequent Smith Guidance and Higgs Guidance; the Government White Paper on modernising Company Law (European Commission, 2003), the Federal Complementary Act to the Swiss Civil Code, 'Obligations Code' chapter (2008).

Significant have been the impacts of the Sarbanes-Oxley Act, particularly for the purpose of imposing a clear and stringent business liability regime and raise the level of 'criminal penalties'.

Unlike in the USA, in other countries, especially the UK, guidelines on corporate governance have been issued for the purpose of introducing exemplary best practices in order to encourage imitation. The Turnbull Guidance issued by Chartered Accountants in England and Wales and the subsequent Smith Guidance and Higgs Guidance had the initial aim of introducing some guidelines on the implementation of the internal audit section of the combined code, and later extending to the areas of corporate governance without ever acquiring the force of law.

In Italy, the main legislation references on this subject were introduced from1997 to 2001:

- Legislative Decree No. 231 of June 8th, 2001, containing 'rules on the administrative liability of corporations', introduced for the first time, in our legal system, criminal liability of companies and their directors for certain types of offences, especially those against the public administration
- Law No. 262/2005, which introduced a number of new provisions on the subject of governance of Italian companies. In particular, it introduced provisions on the subject of liability and obligations relating to corporate disclosures (similarly to the provisions of Sections 302 and 404 of the US Sarbanes-Oxley Act of 2002)
- Commissione Nazionale per le Società e la Borsa (Consob, that is the public authority responsible for regulating the Italian securities market) recommendations (Memo of February 20th, 1997) on the subject of corporate control
- Finance Consolidated Act (Legislative Decree No. 58/1998), which establishes the duties of statutory auditors on the subject of supervision and internal audit
- Code of Conduct of the Italian Stock Exchange
- instructions by Bank of Italy regarding the internal controls system
- Legislative Decree No. 231 of June 8th, 2001 (as amended) on the subject of companies' administrative liability.

In particular, Legislative Decree No. 231 (2001) introduced for the first time in Italian legal system the criminal liability of entities in addition to that of individuals who have physically committed the offense. This decree is the result of the transposition by the Italian legislator as imposed by the European Union. The European Community, sensitive to these issues, has recommended to Member States to introduce into their legal systems specific forms of liability which were going to directly affect legal persons for unlawful acts within criminal law, committed in their organisations and generating a direct economic benefit for the same (D'Agnolo, 2008).

Three conventions touched the problem: the first signed in Brussels on 26 July 1995, a second one 1997 on combating bribery of officials EEC, and then the Second Protocol on the protection of the financial interests of the European Communities, which requires Member States to set the liability of legal persons trough a proper statute.

This leads to the SI No. 300 of 2000, where the Art. 11 provides for the configuration of a system of sanctions of 'administrative' liability of collective entities, in addition to

the forecast of the requirements, conditions and procedures for the recognition of liability and the imposition of sanctions.

The expansion of the liability aims to engage in punishing certain criminal offenses, the assets of entities and, ultimately, the economic interests of the members (Domenichini, 2010).

This regulatory innovation implies the necessity of areal involvement of those persons and stakeholders(partners, associates, etc.) participating in the events of the organisation, in order to control the regularity and legality of the management procedures.

With subsequent regulatory action, the Italian legislature has for example expanded the range of crimes under consideration, including:

- bribery offenses
- fraud against the public administration
- corporate crimes
- offences related to public financing
- organised crime
- offences related to health and safety on workplaces
- crimes of money laundering, receiving and using goods or assets of illicit origin
- terrorism acts
- environmental offenses
- offences related to immigration
- breach of copyright, patents and industrial exclusive
- commercial frauds
- offenses under food safety legislation
- mafia-related offences and arms trafficking
- financial crimes and over stamp duty
- computer fraud offenses market manipulation disclosing confidential information
- bribery offenses between private individuals.

For large part of these crimes, where committed, the contractor may be banned from contracts and subcontracts in the event of competitive bids for concessions and public works contracts.

Adopting an holistic corporate governance system and an IRM model appears therefore crucial (Domenichini and Zambonini, 2010). Decision-making processes should therefore address systematically the risks that are related to the strategic, financial, and operational aspects of the company, particularly when these are linked to the domain of liability.

Besides legal requirements, establishing a proactive risk management approach – a cultural approach – is essential. It is a known fact that certifications are not sufficient to

ensure the presence of an effective organisational model for the prevention of risks and crimes. In Italy, for example, the Ministry of Labour has produced the circular Prot15/VI/0015816/MA001.A001 of July 11, 2011, which draws a line of demarcation between certified management systems and organisational models (DL 231). It stated very clearly that an organisational model 231 – effective for the prevention of risks and crimes – cannot be guaranteed solely by the presence of a certified management system. Therefore, there is a need of a proactive and effective integration among management approaches, regulations and ad-hoc mechanisms for their observance.

Different strategic perspectives should be combined in a governance system. Besides cultural and managerial approaches related to the issues of liability, there is also, for example, the management of safety, quality, health, environment, corporate social responsibility and many others. The related certifications – which are, in order, DL 231, UNI-EN ISO 9001, OHSAS18001, ISO14001, SA 8000 – are therefore necessary but not sufficient.

The lack of this integration can create problems, like the overlapping of regulations, policies and procedures, increasing the paperwork, and replicating controls. Sometimes, there could be also a potential conflict among all the above aspects. These problems, besides being a considerable source of additional costs, slow down procedures, hinder their observance, and they also undermine the effectiveness and efficiency of the system itself.

The lack of effectiveness and efficiency undermines the suitability of the organisational system in the prevention of strategic, financial and operational risks and crimes.

In Italy, since the coming into force of Legislative Decree 231, many consulting firms and freelance professionals have tried to provide a wide range of managerial approaches and tools, that often remain subjective and represent partial interpretations of the legislation.

This has meant that there are common organisational procedures for risk and crime prevention, and especially tools that do not provide integration between systems, nor provide any certainty in communicating activities and their ongoing concrete monitoring.

The result is a considerable amount of paperwork, not always easy or clear, which often remains incomplete (Farrel, 2010).

In addition, we should note that large part of these tools, that are available on the market, follow a 'silos approach' and are the result of specific expertises without an enterprise-wide vision.

There is therefore the need to identify integrated models, in order to compensate the limits resulting from such functional approaches.

4 Towards an integrated approach to the management of liability

Cloud systems and services can represent helpful tools for sharing decision-making process and controls among different actors involved, like managers (in different functions, divisions and headquarters) and external partners (the supervisory board).

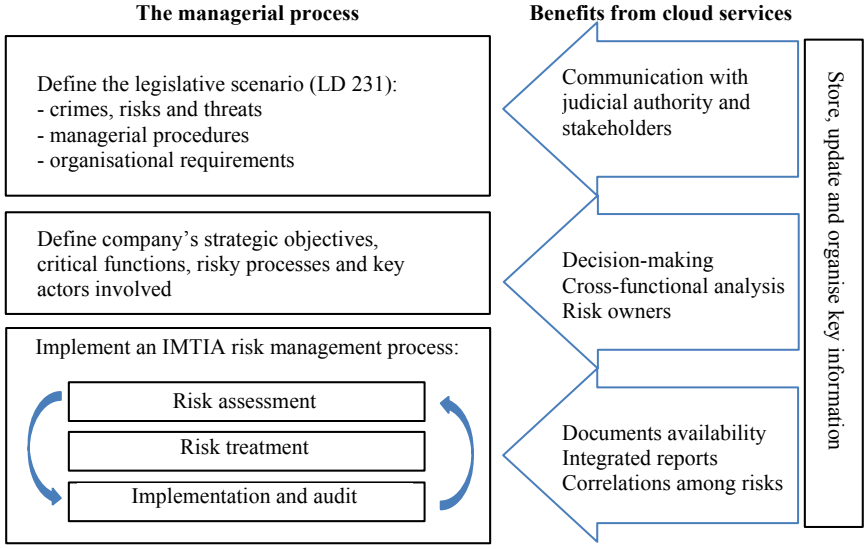
A cloud-based governance system should be oriented towards a web-based application for mapping risky activities, and allows to manage effectively and efficiently business responsibilities, constantly making available important documents to monitor obligations and deadlines in terms of liability requirements. This in order to efficiently

manage bargaining with the public administration. In addition, if one crime were committed, the judge, during the investigation on the suitability of the organisational model, would easily find significant shortcomings in the effective implementation of the rules contained in the model and in the procedures that are implemented.

A pre-requisite for implementing such a governance system is at first to carefully and properly define strategic goals and critical business functions. Hence, it should select key data and documents from different business areas. Then, the system should run the assessment sessions for a detailed mapping of confidential activities in order to put in place all the actions necessary to prevent risks.

The critical steps in building an integrated approach to the management of liability are here described and represented in Figure 1.

Figure 1 The managerial process and the benefits from cloud services (see online version for colours)



A cloud-based governance system should support the management and continuous control of an 'IMTIA' process, which comprehends the following phases (ISO 31.000, 2009):

- identification of all the sensible activities split by areas of processes in which crimes and/or adverse events can emerge or can be committed
- measurement and evaluation of what identified and listed as 'bad or good governance' factors
- treatment, defined and recorded in a specific detailed report with a related deadline, that is linked to risk owners, that is responsible to adequate and mitigate the 'bad governance' factors and their sources
- implementation of new activities/processes to prevent and/or reduce the frequency and/or the severity

- audit of the entire managerial system or part of it, on the basis of a specific request or when the legislative body will require a new update.

The preparation of any database in management systems is the starting point in order to achieve useful results and to proceed with the subsequent steps, such as the definition of resources and procedures to any activity.

From this perspective it is essential to assure 'credibility' to data. The term 'credibility' refers to the level of confidence and trustability that data and documents must have. So then more credible they are then better will be the results, both in the assessment phase or in the treatment decisions.

With respect to the compliance to the LD 231, a could-based governance system may therefore allow for the integration of risk management procedures into the corporate governance system, in order to better assess different risks, to analyse risk exposures, and to adopt risk treatment solutions (Paolozzi, 2006; Thomas et al., 2009). The benefits of a cloud-based integration are therefore related to the capability to keep remotely a constant control over different management systems.

In particular, a cloud-based governance system can safely organise, store and update the following data, assuring also availability for different internal users (managers) and external users (supervisory body):

- risk statistics and measurements
- key activities and processes maps
- operational procedures
- deadlines
- assessment of key risks (identification, measurement and evaluation)
- documents and communications
- staff, operating roles and responsibilities connected
- certification systems manuals
- risk treatment solutions (preventions and mitigations in place).

In addition, a cloud system may allow managers to directly manage and monitor risk-exposed processes, which are related to those inter-functional areas that can represent potential sources of risks and crimes, like for example:

- individual protection devices
- equipments
- injuries at work
- calls for tenders
- training staff.

These data, information and relevant documents should be integrated into a unique system, with ad-hoc tools for the dynamic analysis of confidential activities and related hazards. Through this integration, the organisational model 231 can be constantly updated, and support decision making.

Remote data and documents' accessibility should always allow amore effective task for the supervisory board.

The system should be hosted in a web platform secured against any unauthorised access with the latest cloud computing technologies, firewalls, and data protection.

Authorised user Id and password should be provided together with customised profiles allowing users to access or edit data according to their users rights.

For this scope, technological equipments should assure the following requirements (Kaufman, 2009):

1 flexibility

2 stability

3 power computing

4 compatibility

5 user friendly [graphic user interface (GUI)].

The effectiveness of such an organisational model depends on the following requirements:

- implement an effective 'IMTIA' process
- represent sensitive activities and their risk degree
- identify who is the risk owner in each specific process
- guide the representation of 'as is' scenarios
- carry out an objective evaluation of performances and risks
- guide the identification and implementation of corrective actions
- allow immediate access to business documents and procedures involved
- control the timing of corrective actions procedures, personal protection equipment, tenders and staff training
- directly manage riskier processes (such as participation in tenders).

As already highlighted, a cloud system can make more immediate and complete any intervention. Consequently, it is more credible having the tool to show its action to any inquiries from of the judicial authority after the allegation on commission of crimes. The system can immediately analyse potentially risk-exposed activities (i.e., harbingers of possible offenses) and compare them with good practices applied in the company, with the standards of certification systems through a careful risk assessment process.

5 Risk assessment and final reports

This kind of risk management model, that is customised for the purpose of the LD 231, can compare business practices with the parameters of sound organisation who base the system of sanctions provided by Art. 10 and 11 of Legislative Decree No. 231/2001. From this comparison, the system should calculate sanctions applicable as potential

measure of risk exposition, where the abstract is opened proceedings against the company for an offense committed in each sensitive area considered in the audit process.

Results from risk assessment, treatment and monitoring process should be described and updated in a detailed report for each confidential activity.

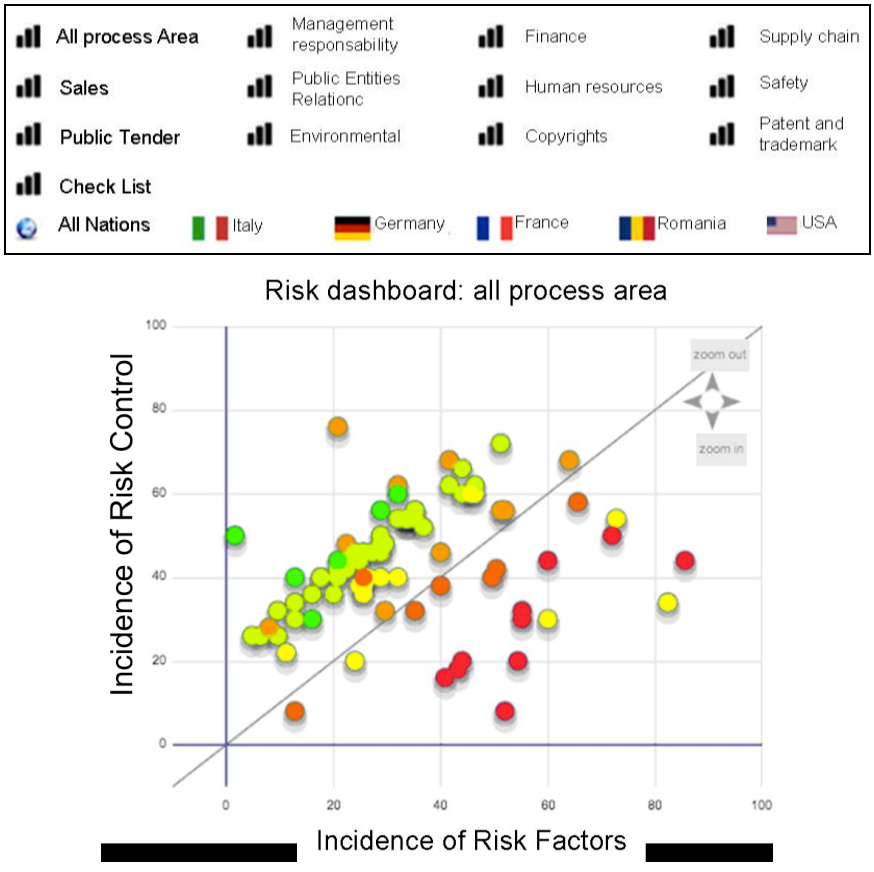
The final output of the analysis should also contain a graphical representation of critical activities and risk sources through a diagram of Prouty (Borghesi and Gaudenzi, 2012). Following this kind of representation, activities should be positioned on the Cartesian plane with the improvement actions and elements of burden. Through a cloud system, the graph could be navigable in the cardinal directions, quickly allowing a deeper analysis of all the points. The placement of the points on the graph can be the expression of the correspondence to the parameters of sound organisation. This representation is possible, like existing risk management models already demonstrate.

Points (key activities) can be coloured on the base of the risk exposure, measurable in terms of sanction that would theoretically applicable if the company were indicted for an offense committed as part considered guilty.

This latter feature is the 'third' dimension of the graph, with the points of different colours (green, yellow and red) in relation to various hypotheses of risk exposition and sanction that can be calculated on the basis of different national legislations.

A representation of the output of this assessment process is shown in Figure 2.

Figure 2 A risk diagram example (see online version for colours)



The system can easily calculate the probable maximum loss (PML) that is the value of the largest loss that is likely to occur (Pirson and Turnbull, 2011). Thanks to the risk control techniques, as loss prevention and loss reduction, the organisation could better control the cost of risk and the risk of being not compliant with the Decree 231.

The overall results should be carefully analysed. The risk analysis model can highlight – for example – the need of an immediate risk reduction that should be evaluated for specific solutions. The process needs always to be verify for its robustness and should be supervised and attended by a representative of the board of directors. During all these risk management sessions, control checklists should be carefully filled, including the analysis of organisational practices based on the statements collected during interviews with key informants in all the processes. Confidential activities differ, for example, depending on the countries where these were carried, and on the amends that are calculated on the basis of local legislation. In fact, in application of Articles 9 and 10 of the Italian criminal code, an Italian company may be penalised for an offense committed abroad, in addition to being sanctioned in accordance with local regulations. Hence, the need for Italian companies that have branches or foreign subsidiaries, to control delicated activities may be carried out abroad based on Italian law is rather that based on the local one.

This management system allows, through the control boards, to consider the sensitive activities carried out in Italy and abroad, and to assess the dangers and the possible sanction, representing these risk drivers in the diagram of dangerousness.

An integrated cloud-based governance system should finally provide detailed reports (DR). Managers could access DRs by clicking on the matching point on the danger diagram, or by selecting it in the process list.

User can also have access to the DR from other pages, such as the general schedule, or the hazard diagram, the organisation diagram, the equipment management system, personal protection equipments, accident registers, training or competitive bidding.

Each DR should contain specific information on risky activities taking into account:

- rules of certification, e.g., ISO9001, OHSAS 18001, etc.
- process areas
- area's reference standards, showing the national boundaries of the rules applied depending on where the considered sensitive activity takes place
- possible deviating action, describing the possible single action that would alter a lawful activity and turn it in an offense
- code of risks and offenses under Italian law
- control or practice, containing a summary of the audit process that involved the indicated function in the organisation chart over the activity considered delicate/risky
- office manager, indicating the position in the organisation of the risk owner
- criteria diagram, containing the ratings as assessed by the auditor to the various parameters linked to the activity in question
- non-conformities management and corrective actions, when the audit process manager identifies non-conformities, giving also the deadline by which they need to

be implemented together with then on-compliance documentation as result of the controlled actions.

6 Conclusions and managerial implications

The complexity of the new legislative scenario and increased stakeholders expectations worldwide impose to companies to manage risks and responsibilities, respecting stringent legal requirements and improving their decision-making processes.

The paper describes the practical example of the Italian regulation in the field of liability of corporation (LD 231), its fundamentals and requirements. From this perspective, authors take some critical steps towards building an integrated approach for governance that can support managers in monitoring critical risks and responding to these legislative requirements.

Risks should be assessed from different perspectives, like the financial, the strategic and the operational. Given these considerations, the paper provides some helpful suggestions in order to identify how to build an integrated governance and risk management system.

Few steps are defined, which are closely related to the most known risk management standards and principles worldwide. The originality of this approach is the measurement of risks in terms of penalties, which can results from the expositions to the risks and crimes established by the LD 231. Moreover, the paper analyses the applicability of cloud-based systems for developing and maintaining this governance and risk management approach. In this perspective, benefits and limitations of cloud-based systems are reported with respect to the specific application of 231.

The first managerial implication is that managing enterprise-wide risks in an integrated fashion is essential in order to protect the companies, and this is confirmed by the Italian regulation on liability. While this principle is well known, the papers can provide directions for moving from theory to action. Through this practical approach, the paper aims also to partially fill an existing gap in the literature about concrete applications of risk assessment.

The second implication is that, besides legal requirements, establishing a proactive risk management approach should be a cultural change, more than a reaction to new regulations.

Legislators highlighted that certifications are not sufficient to ensure the presence of an effective organisational model for the prevention of risks and crimes. Contrarily, certifications without a proactive organisational change can create confusion, conflicts and useless paperwork.

The third implication is that cloud-based systems can be helpful tools for sharing information and supporting decisions, but cannot substitute decision makers. Strategic goals, critical functions and key risks should be established through robust process mapping and procedures, before implementing cloud computing services systems. Otherwise, these IT solutions can create risks instead of contributing to control them.

After this first study, authors aim at developing this approach in depth, testing it with a sample of companies in order to validate its applicability.

References

AIRMIC, ALARM and IRM (2010) *A Structured Approach to Enterprise Risk Management (ERM) and the Requirements of ISO 31000*, Standard Report.

Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. and Zaharia, M. (2010) 'A view of cloud computing', *Communications of the ACM*, Vol. 53, No. 4, pp.50–58.

Bandyopadhyay, K., Mykytyn, P.P. and Mykytyn, K. (1999) 'A framework for integrated risk management in information technology', *Management Decision*, Vol. 37, No. 5, pp.437–445.

Bartolomucci, S. (2004) *Corporate governance e responsabilità delle persone giuridiche*, IPSOA, Assago-Milano.

Benlian, A. and Hess, T. (2011) 'Opportunities and risks of software-as-a-service: findings from a survey of IT executives', *Decision Support Systems*, Vol. 52, No. 1, pp.232–246.

Borghesi, A. and Gaudenzi, B. (2012) *Risk Management. How to Assess, Transfer and Communicate Critical Risks*, Springer, Milano.

Brawn, L. and Caylor, M. (2004) 'The correlation between corporate governance and company performance', *Institutional Shareholders Services*, Vol. 31, No. 1, pp.31–55.

Christopher, M. and Gaudenzi, B. (2009) 'Exploiting knowledge across networks through reputation management', *Industrial Marketing Management*, Vol. 38, No. 2, pp.191–197.

Copeland, T., Koller, T. and Murrin, J. (1996) *Valuation: Measuring and Managing the Value of Companies*, 2nd ed., John Wiley & Sons, New York.

D'Agnolo, M. (2008) *Commento al Decreto Legislativo 8 Giugno 2001 n. 231 (responsabilità amministrativa degli enti) per Istituto di Studi sulla Responsabilità Amministrativa degli Enti – 2008* [online] http://www.cloudgovernance.it/documents/Commento%20al%20decreto%20legislativo%208%20giugno%202001.pdf (accessed 21 June 2013).

Daccò, G. (2004) *L'organizzazione aziendale*, CEDAM, Padova.

Dickinson, G. (2004) 'Enterprise risk management: its origin and conceptual foundation', *Geneva Paper Risk Insurance*, Vol. 26, No. 3, pp.360–366.

Domenichini, P. (2010) *Verso una centralità dei modelli organizzativi nelle strutture di compliance*, Istituto di Studi sulla Responsabilità Amministrativa degli Enti [online] http://www.cloudgovernance.it/documents/commentosentenzamilano.pdf (accessed 21 June 2013).

Domenichini, P. and Zambonini, V. (2010) *Il caso Telecom Italia*, Istituto di Studi sulla Responsabilità Amministrativa degli Enti [online] http://www.cloudgovernance.it/documents/Commento%20al%20caso%20Telecom%20Italia (accessed 21 June 2013).

Elgharbawy, A. and Abdel-Kader, M. (2013) 'Enterprise governance and value-based management: a theoretical contingency framework', *Journal of Management and Governance*, Vol. 17, No. 1, pp.99–129.

Emblemsvåg, J. (2010) 'The augmented subjective risk management process', *Management Decision*, Vol. 48, No. 2, pp.248–259.

ERM Framework (2004) [online] http://www.coso.org/documents/coso_erm_executivesummary.pdf (accessed 21 June 2013).

Fama, E.F. and Jensen, M.C. (1996) 'Separation of ownership and control', *Journal of Law Economics*, Vol. 26, No. 2, pp.301–325.

Fan, M., Kumar, S. and Whinston, A.B. (2009) 'Short-term and long-term competition between providers of shrink-wrap software and software as a service', *European Journal of Operational Research*, Vol. 196, No. 2, pp.661–671.

Farrel, R. (2010) 'Securing the cloud-governance, risk, and compliance issues reign supreme', *Information Security Journal: A Global Perspective*, Vol. 19, No. 1, pp.310–319.

Ferrari, A., Rossignoli, C. and Mola, L. (2012) 'Organizational factors as determinants of SaaS adoption', *Information Systems: Crossroads for Organization, Management, Accounting and Engineering*, pp.61–66, Physical-Verlag HD, Berlin.

Gatewood, B. (2009) 'Clouds on the information horizon: how to avoid the storm', *Information Management Journal*, Vol. 43, No. 4, pp.32–36.

Gens, F. (2008) *IT Cloud Services User Survey, Part 1: Crossing the Chasm*, IDC Xchange [online] http://tinyurl.com/4mu7qx (accessed 21 June 2013).

Gold, J. (2012) 'Protection in the cloud: risk management and insurance for cloud computing', *Journal of Internet Law*, Vol. 15, No. 12, pp.1–28.

Gold, N., Mohan, A., Knight, C. and Munro, M. (2004) 'Understanding service-oriented software', *IEEE Software*, Vol. 21, No. 2, pp.71–77.

ISACA (2009) *IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud* [online] http://www.isaca.org/Knowledge-Center/Research (accessed 21 June 2013).

Jones, C., Hesterly, W.S. and Borgatti, S.P. (1997) 'A general theory of network governance: exchange conditions and social mechanisms', *Academy of Management Review*, Vol. 22, No. 4, pp.911–945.

Kaufman, L. (2009) 'Data security in the world of cloud computing', *IEEE Internet Computing*, Vol. 7, No. 4, pp.61–64.

Mell, P. and Grance, T. (2009) *The NIST Definition of Cloud Computing* [online] http://csrc.nist.gov/groups/SNS/cloud- computing/cloud-def-v15.doc (accessed 21 June 2013).

Mola, L. and Carugati, A. (2012) 'Escaping localisms in IT sourcing: tracing changes in institutional logics in an Italian firm', *European Journal of Information Systems*, Vol. 21, No. 4, pp.388–403.

Paolozzi, G. (2006) *Vademecum per gli enti sotto processo*, Giappichelli, Milano.

Pirson, M. and Turnbull, S. (2011) 'Corporate governance, risk management, and the financial crisis: an information processing view', *Corporate Governance: An International Review*, Vol. 19, No. 5, pp.459–470.

Premkumar, G., Ramamurthy, K. and Saunders, C.S. (2005) 'Information processing view of organizations: an exploratory examination of fit in the context of interorganizational relationships', *Journal of Management Information Systems*, Vol. 22, No. 1, pp.257–294.

Rahim, M. (2012) 'The new governance approach to the devolution of corporate governance', *Competition and Change*, Vol. 16, No. 4, pp.343–352.

Thomas, R.J., Schrage, M., Bellin, J.B. and Marcotte, G. (2009) 'How boards can be better: a manifesto', *Sloan Management Review*, Vol. 50, No. 5, pp.44–50.

Walterbusch, M., Martens, B. and Teuteberg, F. (2013) 'Evaluating cloud computing services from a total cost of ownership perspective', *Management Research Review*, Vol. 36, No. 6, pp.613–638.