Risk Management in IT Governance Framework

Mirela GHEORGHE[1]

ABSTRACT
The concept of governance has an already old contour: the system by which business corporations are directed and controlled. The most praised principles regarding shareholder rights, transparency and board accountability now constitute the foundation for new tendencies evolved from such ground. Executive compensation, transparency and shareholder reporting are new issues attached to board responsibilities. Besides such almost negative approaches the board faces a more and more prominent role from risk management and IT governance perspective. Nowadays is generally acknowledged that the board is in charge for managing and controlling the risks to assets of the enterprises and business future. IT Governance has emerged as a support for corporate governance, as an important part of board's striving efforts to perform better in a competition environment. These responsibilities, risk management and IT Governance, remain within the framework of old concept of corporate governance and are fed from its substance. The interaction between these concepts is the core interest of this research.
IT Governance is defined as procedures and policies established in order to assure that the IT system of an organization sustains its goals and strategies. The management of the organisations face a new challenge: structural redefinition of the IT component in order to create plus value and to minimize IT risks through an efficient management of all IT resources of the organisation. The evolution of the present IT environment is a natural process according to which business environment should adapt.

KEYWORDS: *Corporate Governance, IT Governance, IT risk, Risk Management.*

JEL CLASSIFICATION: *M15*

INTRODUCTION

In specialists Michael Crouhy, Dan Galaia and Robert Mark's opinion, risk management offers the grounds for creating a complete and coherent integrated management system, by generating efficient risk management strategies. This process reinforces any organization's corporate management, by taking into account the existing technological infrastructure, the adopted control strategies and investment solutions. (Crouhy, Galai & Mark, 2001)

Risk management is considered to be an integrated part of any organisation's management (Ciocoiu, 2008), whose objective is risk identification, analysis and evaluation, with the purpose of implementing additional control measures that lead to risk reduction. In other words, the goal of risk management is reducing the organisation's vulnerability to ill environment changes, and by this reaching the fixed objectives with maximum efficiency.

[1] The Bucharest Academy of Economic Studies, Romania, mirelaghe@gmail.com

The present paper's purpose is to approach the complex problem of risk management, under the premise that risk must be treated as a conscious and calculated assumption of reality. Within this context, research tries to answer the following questions: which are the principles of corporate governance and in what measure does it continue to exist in the new reality generated by the world economic crisis? Which are the ares of interest for IT governance and what is the risk management process 'position? Which is the content of this process?

In an attempt to answer these questions, the applied methodology is based on the analysis of specialized literature, so that we may say that the accomplished operations will hold a place in the area of descriptive research.

1. CORPORATE GOVERNANCE CONCEPTUAL FRAMEWORK

It is helpful to recall and put clearly in words the purposes of Corporate Governance. The Financial Reporting Council (FRC) Combined Code sets out the purpose of Corporate Governance as follows:
"Good corporate governance should contribute to better company performance by helping a board discharge its duties in the best interests of shareholders; if it is ignored, the consequence may well be vulnerability or poor performance. Good governance should facilitate efficient, effective and entrepreneurial management that can deliver shareholder value over the longer term" (Financial Reporting Council, 2008).

This view is underlined by the preamble to the OECD's Principles of Corporate Governance, which sets out clearly the importance of Corporate Governance as its follow:
"The presence of an effective corporate governance system, within an individual company and across an economy as a whole, helps to provide a degree of confidence that is necessary for the proper functioning of a market economy. As a result, the cost of capital is lower and firms are encouraged to use resources more efficiently, thereby underpinning growth." (OECD, 2004).

Corporate Governance promotes not only principles beneficial for the economy as a whole, but also solution for ensuring that there are effective controls that help to identify shortcomings and failures in corporate activities. This view of Corporate Governance goes back at least as far as the Cadbury Report:
"Had a Code such as ours been in existence in the past, we believe that a number of the recent examples of unexpected company failures and cases of fraud would have received attention earlier" (Cadbury, 1992).

There are two conflicting philosophical arguments: the first, or what might be described as Corporate Governance-lite approach, is as follows: Corporate Governance is there to enable boards to discharge their duties as best they can in the light of prevailing conditions, but if the conditions are not favorable, then the board should not be held accountable because events were outside their control. In the case of the current Financial Crisis, no-one, within organizations or within the regulatory or political environment foresaw the problems, and as a consequence, no matter how good the Corporate Governance arrangements, no different outcome could have been expected.

The second, countervailing argument would run as follows: Boards have a responsibility to identify and understand the conditions within which their organisations are operating, to ensure that there is alignment between long and short term strategy, to ensure that

remuneration policies are in line with the long term strategy, that ethical standards, risk management and assurance practices are appropriate so as to identify potential issues as soon as possible. Irrespective of the crisis, boards should have been evaluating the developing conditions and should have been cognizant of their responsibilities to a broader concept of society.

Under the first description of Corporate Governance, one would be examining whether different models of Corporate Governance would have made a difference. Under the second description, we would be examining whether there are improvements that can be made to Corporate Governance arrangements, which would help to prevent or at least alleviate the worst impacts of the Financial Crisis. If you adopt the first description of Corporate Governance, then the questions are purely about the board, its composition and its committees. If you adopt the second description, then the debate enlarges and becomes about how the tone and approach adopted at the board level are translated into the day-to-day activities of the organization.

2. IT GOVERNANCE AND RISK MANAGEMENT

Significant literature in governance area reveal that government processes can be lined up in three groups: Enterprise Governance, Corporate Governance, and IT Governance.

Enterprise Governance has been described as "the set of responsibilities and practices exercised by the Board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly (ITGI, 2001)

Corporate Governance has been defined as "the ethical corporate behaviour by directors or others charged with governance in the creation and preservation of wealth of all stakeholders" (Weill & Ross, 2004). The Australian Stock Exchange Corporate Governance Council considers corporate governance to be "the systems by which companies are directed and managed. It influences how the objectives of the company are set and achieved, how risk is monitored and assessed, and how performance is optimized" (ASX, 2003).

IT Governance has been defined by the ITGI "IT governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organisational structures and processes that ensure that the organisation's IT sustains and extends the organisation's strategy and objectives" (ITGI, 2001).

Van Grembergen defines IT Governance as follows: "IT governance is the organisational capacity exercised by the board, executive management and IT management to control the formulation and implementation of IT strategy and in this way ensure the fusion of business and IT" (Van Grembergen, 2002).

Literature contains many other definitions. Despite the apparent disagreement between scholars, the IT Governance definition stressed "the red thread" that IT should sustain the organization objectives.

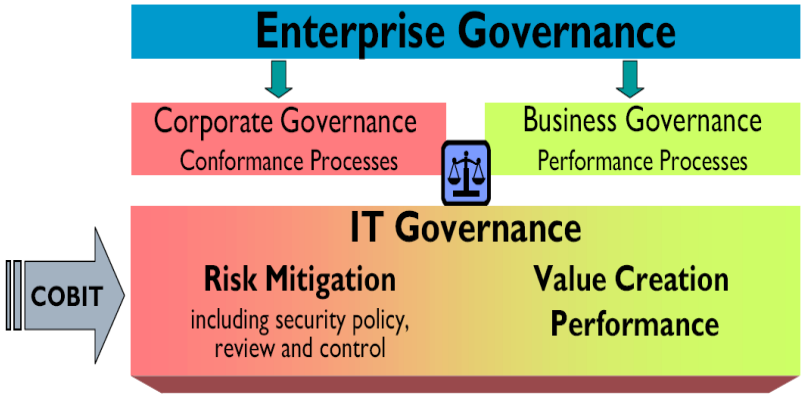

Figure 1. Relation between Enterprise Governance, Corporate Governance and IT Governance
Source: IGSI, 2005

Van Grembergen's definition reveals that IT management remains a main actor within the IT Governance processes. Despite the association between IT management and IT governance, the two concepts remain different. IT management is in charge with providing effective IT services, with supplying and management of IT services and products. On the other hand IT governance is much broader and focuses on performing and transforming IT to meet demands of the business and the business' customers.

IT Governance Institute reveals that IT governance is part of much broader notion of Corporate Governance. Lining up in this order the two concepts, IT governance should follow the principles of corporate governance, i.e. effective, transparent and accountable.

IT Governance reflects broader corporate governance principles while focusing on the management and use of IT to achieve corporate performance goals. Because IT outcomes are often hard to measure, firms must assign responsibility for desired outcomes and assess how well they achieve them. IT Governance shouldn't be considered in isolation because IT is linked with other key enterprise assets (financial, human, intellectual property etc). Thus, IT Governance might share mechanisms (such as executive committees and budget processes) with other asset governance processes thereby coordinating enterprise wide decision making processes (Weill & Ross, 2004).

3. IT GOVERNANCE FOCUS AREA

In practice IT Governance supports the business, adding plus value through IT component and IT risks minimisation. In order to achieve such purposes IT Governance should cover five principal domains (in ISACA vision (ITGI, 2001)):

- IT Strategic alignment
- Value delivery
- Risk management
- Resource management
- Performance measurement

3.1. Aligning IT strategy with business strategy

This first domain of IT Governance has the starting point in designing an IT strategy according with the overall strategy of the organisation. Thus, starting to the organisation's strategic plan IT strategy committee should lay down an IT strategy in line with the business objectives. In particular, IT governance practices should:

- ensure that IT strategy is aligned with business strategy
- ensure that IT delivers against the strategy through clear expectations and measurement
- allocate IT investments budgets in accord with the business objectives
- ensure that technology investment decisions are aligned with business goals.
- provide high-level direction to create competitive advantages that parallel compliance processes
- direct IT strategy by addressing the level and allocation of investments, balancing the investments between supporting and growing the enterprise and by making considered decisions about where IT resources should be focused
- ensure a culture of openness and collaboration among the business, geographical and functional units of the enterprise.

3.2. Value Delivery

Starting from the premises of the corporate governance, underlining that "a company, in first place, have to aim the maximization of the value of their shares on long term", the implementation of the new IT techniques have to add value to organization by the quality of the services, expenses optimization, offer of pertinent and useful data delivered timely. IT value delivery is defined as "delivery on time, within budget and with the benefits that were promised. In business terms, this often translates into: competitive advantage, elapsed time for order/service fulfilment, customer satisfaction, customer wait time, employee productivity and profitability" (ITGI, 2001).

IT Governance should target a proper quality of the IT services combining the resources from the budget and the time factor.

The governance practices for IT value delivery are:

- ensure that IT plans proceed on schedule
- ensure the completeness, quality and security of IT investments
- monitor IT investments for adequate returns
- ensure bankable benefits through IT services.

3.3. Resource Management

IT resource management is concerned with the management of IT resources and the organisation of IT infrastructures within a corporation. This critical dimension of IT Governance processes aims to provide high level direction for sourcing and use of IT resources, to oversee the aggregate funding of IT at the enterprise level and to ensure that there is adequate IT capability and infrastructure to support current and expected future business requirements (Hardy, 2003). Another important aspect of this domain is the issue of project management. Management of new IT projects must be properly governed as these projects have considerable impact on the financial position and strategic direction of the organization.

The governance practices for IT resource management are the following:

- allocate IT resources in correlation with business priorities
- implement adequate controls which allow to identify over fulfilled IT infrastructures
- sustain an adequate investment in staff education, development and training for IT operations and developments

3.4. Risk Management

Specialized authors define in their writings risk management as being "the process of identifying the vulnerabilities and threats from the framework of an organization as well as designing procedures in order to minimize the impact of them on IT resources". The risk on organization level cannot be eliminated; it will exist all the time; the management of the organization is responsible with minimizing it to an acceptable level. Risk management should be a continuous process which begins by assessing the level of exposure of the organization and identifying the main incident risks. Once identified, risks have to be minimized using control procedure and finally residual risk should be adjusted at acceptable level.

We will underline that the governance practices for IT risk management are:

- analyze and asses IT risks
- monitor efficiency of internal controls
- implement necessary controls to minimize IT risks
- put in place procedures to ascertain the transparency about the significant risks to the enterprise
- consider that a proactive risk management approach can create competitive advantage
- Insist that risk management be embedded in the operation of the enterprise
- Ascertain that management has put processes, technology and assurance in place for information security to ensure that:
  - Business transactions can be trusted
  - IT services are usable, can appropriately resist attacks and recover from failures
  - Critical information is withheld from those who should not have access to it.

3.5. Performance Measurement

Performance measurement is concerned with determining whether IT systems have achieved the goals set for them by the Board and senior management. For IT performance measurement, IT governance practices should:

- Define and monitor measures together with management to verify that objectives are achieved
- Measure IT performances through metrics, adequate indicators.

Implementing the IT Governance framework any organization should balance internal factors as well as external relevant factors, such as:

- *The fact of technological development:* The fast development of the domain requires that decisions related to IT be made on a timely basis, with full understanding of the risks associated with the IT challenges.

- *The fiscal scrutiny:* Large IT projects need expensive spending causing sometimes doubt and accountability for discretionary waste of financial resources.
- *Innovation and control over IT:* In cases where the innovation (new IT projects) is supported by IT, it may run counter to the objective of exerting control over the IT environment.
- *Up to date infrastructure:* Technology infrastructure becomes out of date over time. Keeping it up to date is a must for every department.

To sum it up, we can state that government practices associated with the five fundamental domains are material factors in the decision making process. Subsequent to objectives self-imposed, IT Governance achieves the alignment of the IT investments with business objectives, assures a responsible use of the IT resources, and assures that IT performances are within the borders of the approved budget and IT strategic plan.

Following its principles IT governance provide a decreasing of the IT risks trough a continuous scrutiny of the threats and weaknesses of the system improves IT organizational performance, compliance, staff development and outsourcing initiatives.

CONCLUSIONS

Not only that the knowledge-based society cannot eliminate the traditional risk concept, but must also accept the necessity of its reconsideration and readjustment to a new informational dimension. In an economy where information technology has enforced itself in all domains of activity, the risk problem receives a special valence and dictates changes within the fundamental principles of risk management.

Modern management needs to be risk-sensitive, pursue the implementation and usage of reliable, performing systems, by elaborating action and security plans by ranking the objectives on operational levels which are adaptable to permanent changes.

The accomplished research is based on a specialty literature analysis, by identifying the risk management process characteristics at a conceptual level, mangers' perception regarding the importance of this process and the need for integration in an organization's governing structures. The recent bankruptcies (Long-Term Capital Management (1998), Enron (2002), Societe Generale (2008), etc) and world economic crisis have intensified the risk management regulatory authorities' efforts with risk management and the result can be seen in the number of methodologies and standards in this field. (Risk Management Institute Standard, ISO 31000, ISO 31010, ISO 27001, Octave Method, NIST Method).

Recent studies (Unit, 2007) reveal that risk management has reached a maturity level and this is transposed by modifying this process' paradigm from simple threat detection to intense benefit increase methods. The actual tendency rather promotes proactive management, which allows for the identification of possible threats, before they materialize and have ill influences over the established objectives. *Proactive Management* is grounded on the "it is better to predict than to treat" principle.

A performing management system will not be limited to the "short term horizon" but will also consider further perspectives. In these situations, proactive management becomes prospective management and means to identify those risks that cannot occur as a consequence of strategy or environment modifications.

ACKNOWLEDGEMENTS

This work was cofinanced from the European Social Fund through Sectoral Operational Programme Human Resources Development 2007-2013, project number POSDRU/89/1.5/S/56287 „Postdoctoral research programs at the forefront of excellence in Information Society technologies and developing products and innovative processes", partner Bucharest Academy of Economic Studies – Research Center for "Analysis and Regional Policies .

REFERENCES

ASX, C. G. (2003). *Principles of Good Corporate Governance and Best Practice Recommendations*

Cadbury, C. (1992). *The Financial Aspects of Corporate Governance, known as The Cadbury Report,* Gee (a division of Professional Publishing Ltd) South Quay Plaza, London

Ciocoiu, C. N. (2008). *Managementul riscului. Teorii, practici, metodologii*, Editura ASE, Bucharest

Crouhy, M., Galai, D., & Mark, R. (2001). *Risk Management,* McGraw-Hill

Financial Reporting Council, F. (2008). *The Combined Code on Corporate Governance*, Aldwych House, London

Hardy, G. (2003). Coordinating IT Governance - A new Role for IT strategy committees, *Information Systems Control Journal*, 4

IGSI, (2005). *The place of IT Governance in the Enterprise Governance,* Institute de la Gouvernance des Systems d'Information

ITGI, (2001). *Board Briefing on IT Governance*, IT Governance Institute, Retrieved from http://www.itgi.org

OECD, (2004). *Principles of Corporate Governance*

Unit, T. E. (2007). *Best practice in risk management*

Van Grembergen, W. (2002). Introduction to the Minitrack: IT Governance and its Mechanisms, *Proceedings of the 35th Hawaii International Conference on System Sciences* (HICSS)

Weill, P., & Ross, J. W. (2004). IT Governance on One Page, *CISR Working Paper*, 349