EFFICIENT RISK MANAGEMENT AND INTERNAL AUDIT

Dr. Theofanis Karagiorgos1, George Drogalas2,*, Dr. Iordanis Eleftheriadis3, Dr. Petros Christodoulou4

Abstract: There is currently considerable interest in the topic of internal audit and its contribution to the effective risk management. The business enterprise—in both the public and private sector is seen as a potent force in our society. Within the framework of extremely fluid business environment, the paper aims at examining the relation between the management’s effectiveness and the efficient risk assessment. In this paper, at first, the conceptual approach of risk is analysed. Then, an integrated categorization of business risk is depicted. After that an audit risk model is presented. Finally we deal with some basic limitations, we analyse the outcomes of the literature review and we suggest areas for further research. The results point out that internal audit is vital in the efficient risk management and consequently in the business survival and success.

Keywords: Risk management, Internal auditing, Audit risk, Inherent Risk, Control risk, Detection Risk, Information Risk

JEL Classification: D81, M40, M10

INTRODUCTION

Rapid changes in information technology and managerial practices in many organizations were forcing efficient risk management as a vital mean for reducing the total business risk. Management uses risk assessment as part of the process of ensuring the success of the entity. In this process, internal audit will be a key player by using modern auditing techniques and specialized audit risk models.

1. Dr. Theofanis Karagiorgos: Associate Professor and Head of the Department of Business Administration, University of Macedonia, Greece. Mailing Address: 156, Egnatia Str., Thessaloniki, Greece Zip Code: GR-540 06, Tel.: 00302310891596, E-mail: karagth@uom.gr.
2. George Drogalas: Ph.D. Candidate, Department of Business Administration, University of Macedonia, Greece. Mailing Address: 156, Egnatia Str., Thessaloniki, Greece Zip Code: GR-540 06, Tel.: 00302310891590, E-mail: drogalas@uom.gr.*: Corresponding Author.
3. Dr. Iordanis Eleftheriadis: Assistant Professor, Department of Business Administration, University of Macedonia, Greece. Mailing Address: 156, Egnatia Str., Thessaloniki, Greece Zip Code: GR-540 06, Tel.: 00302310891591, E-mail: jordan@uom.gr.
4. Dr. Petros Christodoulou: Associate Professor, Department of Business Administration, University of Macedonia, Greece. Mailing Address: 156, Egnatia Str., Thessaloniki, Greece Zip Code: GR-540 06, Tel.: 00302310891592, E-mail: christod@uom.gr.
Through an extended literature review, there will be an attempt to approach theoretically internal audit’s catalytic contribution to the efficient risk management. The purpose of this paper is brought to light the resulting bunch of benefits of internal control in the modern business environment.

The incentive for this paper reflects an aspiration to examine and enrich the significance of internal control in the effective risk management. Until now, no similar integrated research on the role of internal auditing in risk management has been conducted within a Greek context. In this study we elaborate in more detail the internal control concept, by pointing out the more important definitions. In these frames, this article attempts to approach theoretically the connection between internal auditing and efficient risk management. Furthermore, it became effort to analyze the significance of risk and the development of risk management systems up to today.

In order to best accomplish our scope, the remainder of this paper is organized as follows: section 2 outlines the necessary theoretical background on the concept of internal audit. Then, section 3 is focused on the concepts of “risk” and “risk assessment”, by mentioning the most important definitions diachronically and section 4 describes a categorization of risk types. In section 5 we attempt to approach the collaboration between risk management and internal audit. To be more in practice, an audit risk model is presented by analysing in detail the components of this model in section 6. Via this model, we attempt to focus on the usefulness of internal control as tool of effective management. The final section formulates conclusions, outlines some major limitations of this study and suggests further areas for research.

**CONCEPTUAL FRAMEWORK OF INTERNAL AUDIT**

Indicative of internal audit’s great importance is the significant amount of definitions that are given by many researchers. In this concept, internal audit has developed gradually on the basis of social and economic development and the inherent needs of enterprise management (Wang, 1997). Furthermore, recent years have witnessed an explosion in the academic literature of auditing history throughout
the world. Internal control has been defined in many international studies and these definitions show great similarities.

According to the Institute of Internal Auditors, (IIA, 1991; Taylor and Glezen, 1991; Konrath, 1996) internal auditing is “an independent appraisal function, established within an organization to examine and evaluate its activities as a service to the organization”. By measuring and evaluating the effectiveness of organizational controls, internal auditing, itself, is an important managerial control device (Carmichael et al., 1996), which is directly linked to the organizational structure and the general rules of the business (Cai, 1997).

Moreover, COSO Framework (1992) and The Turnbull Report (1999) defines internal audit: The system of internal control comprises those elements of an organization that support people in the achievement of the organization's objectives. They facilitate the effective and efficient operation of companies by enabling them to respond appropriately to significant business, operational, financial, compliance and other risks. This includes safeguarding assets from inappropriate use or from loss and fraud, and ensuring that liabilities are identified and managed. Furthermore, internal controls help to ensure the quality of internal and external reporting, which also includes procedures for reporting immediately to appropriate levels of management of any significant control failings or weaknesses that are identified together with details of corrective action. Finally, internal controls help to ensure the compliance with applicable laws and regulations (Sarens and Beelde, 2006).

In the meantime the Canadian Institute of Chartered Accountants has provided a definition for control (Canadian Institute of Chartered Accountants, 1995) which reflects a much broader approach to control and risk, directly related to organizational objectives.

More recently, Papas (1999) argue that internal audit, being an independent department, is an important means for an enterprise to strengthen operational management. In this concept, Jou (1997) argued that, internal control system is not only a significant part of the modern enterprise system, but also an important way that enterprises
emphasize on better management and enhance economic benefits, substantially embodying the self-restraint system of enterprises.

In June 1999, the Institute of Internal Auditors (IIA) officially adopted a new definition of the internal auditing function, which defines the internal audit function as: “an independent, objective assurance and consulting activity designed to add value and improve an organization’s operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes (IIA, 2000). The new definition shifts the focus of the internal audit function from one of assurance to that of value added and attempts to move the profession toward a standards-driven approach with a heightened identity (Bou-Raad, 2000; Krogstad et al., 1999; Nagy and Cenker, 2002; Karagiorgos et al., 2006; 2007).

From the above, it is important to stress that a sound system of internal control provides reasonable, but not absolute, assurance that a company will not be hindered in achieving its business objectives by circumstances which may reasonably be foreseen (Sarens and De Beelde, 2006).

**RISK AND RISK ASSESSMENT**

Risk has many concepts and is inherent in the activities of most organisations. Risks come from current activity, from changes in the external environment, and from the related decisions of the management.

According to Selim and McNamee (1999b) risk is defined as “a concept used to express uncertainty about events and/or their outcomes that could have a material effect on the goals and objectives of the organization”. In the modern enterprise new risks are created (Sarens and De Beelde, 2006). More recently, Bekiaris (2003) considered risk as the report of an entity in uncertain changes.

The key activity with respect to risk is to manage it. Selim and McNamee (1999a) argued that this starts with a risk assessment where the organization attempts to estimate the probable consequences of threats and opportunities (risk identification, measurement and
prioritization), followed by risk management, where decisions need to be made about how to manage the perceived consequences of that risk.

As we said business risk assessment is the first stage which is designed to give a top-down, business-risk orientation to audit work (Bell et al., 1997). Risk assessment is an ongoing and integral responsibility of management, because management can not establish objectives and simply assume that they will be achieved and all the time new risks deviate from the internal and external business environment (Sawyer, 2003). The new approach is intended to provide valuable insights and information to management (Crawford and Stein, 2002). According to Williams (1995) risk identification is the most important stage in the assessment.

Risk management which is the second stage, is a newer field. The term was first pop up in the 1950s by large American corporations seeking alternatives to costly or inadequate insurance cover. Risk management covers the identification and mitigation of risks which may prevent an organisation from achieving its objectives. Risks can be managed to acceptable levels by:

- transferring them to other parties (such as suppliers, investors)
- controlling them by applying appropriate internal control policies and procedures;
- avoiding them.

CATEGORIZATION OF RISK TYPES

Every company faces different risks, based on its business, economic, social and political factors, the features of the industry it operates in, state of industry relations, capabilities of its staff, and other innumerable factors. A list of the most important categories of risks in detail is stated below (Eleftheriadis et. al, 2008; Pazarskis et. al, 2007; Eleftheriadis, 2006; Olsson, 2002):

- **Business risk** is the risk of failing to achieve business targets due to inappropriate strategies, inadequate resources or changes in the economic or competitive environment.
- **Credit risk** is the risk that a counterparty may not pay amounts owed when they fall due.
- **Market risk** is the risk of loss due to changes in market prices. This includes
• Interest rate risk
• Foreign exchange risk
• Commodity price risk
• Share price risk
• Liquidity risk, the risk that amounts due for payment cannot be paid due to a lack of available funds.
• Operational risk, the risk of loss due to actions on or by people, processes, infrastructure or technology or similar, which has an operational impact including fraudulent activities.
• Accounting risk, the risk that financial records do not accurately reflect the financial position of a company.
• Industry risk is the risk associated with operating in a particular industry.
• Environmental risk, the risk that a company may suffer loss as a result of environmental damage caused by themselves or others which impacts on their business.
• Legal/regulatory risk is the risk of non-compliance with legal or regulatory requirements.
• Systemic risk is the risk that a small event will produce unexpected consequences in local, regional or global systems not obviously connected with the source of the disturbance.
• Reputational risk is the risk that the reputation of a company will be adversely affected.
• Audit risk is the risk where exists the probability to do not evaluate and contribute to the improvement of risk management, control and governance or do not recognize the assurance and consulting role of internal auditing in corporate governance and simultaneously in risk assessment. This includes
  - Inherent Risk
  - Control Risk
  - Detection Risk
• Information risk is the risk that unreliable information will be provided to decision makers (Arens and Loebbecke, 1991).

LINKING INTERNAL AUDITING AND RISK MANAGEMENT

For more than a decade, risk management in general, and internal control more specifically, have been considered as fundamental
elements of organizational governance. However the relation between risk management and internal auditing remains confused.

The COSO framework considers risk assessment as one of the five components of internal control. In COSO report (Coso, 1992), risk assessment was first considered as constitutive element of internal control (Rezaee, 1995) that help in the harmonious adoption and efficient operation of internal auditing. More analytically the five basic elements of internal auditing were considered (Messier, 1997, Knechel 2007):

- Control environment- the circumstances of the client
- Risk assessment - the ability to identify threats
- Control activities - the actions taken to intervene
- Monitoring - the maintenance of controls and
- Information and Communication - the ability to coordinate it all.

It is worth noting at this point that previous control frameworks issued in the US and Canada included risk assessment and risk management activities as part of internal controls. Later the Canadian Institute of Chartered Accountants (1995, p.9) perceived control as encompassing risk (Spira and Page, 2003)

The Turnbull report is the first public document, relating to UK, to emphasize the relation internal control and business risk. On the contrary Cadbury did not explicitly link the two concepts. In the meantime Coso report identified risk assessment as one of the five components of internal control.

An important step was the new definition of Internal auditing issued by the IIA in June 1999, which clearly states that “the internal auditing activity should evaluate and contribute to the improvement of risk management, control and governance” (IIA, 1999).

To verify the above events, Chambers (2000) observed the increasing references to risk (management) over the last five years in professional journals related to internal audit.

Moreover, over 60 percent of the respondents of a KPMG survey (2002) in eight European countries believed that their systems of risk management and internal control add value to their organization.
More recently, the Leung et al. (2003)’s large-scale study within Australian companies revealed that a large majority of internal auditors regarded risk management (74 percent) and internal control (91 percent) as important internal audit objectives.

Moreover, the Institute of Internal Auditors, IIA (2004), by stating that the internal audit activity should evaluate and contribute to the improvement of risk management, control and governance, recognizes the assurance and consulting role of internal auditing in corporate governance and simultaneously in risk assessment.

Finally, according to Beumer (2006) risk management and internal auditing use the same tools and methodology:

- Risk maps that quantify the risk exposures.
- Objectives and strategy used as a starting point for risk assessment.
- Risk reporting to relevant management levels and the board.
- Action plans defined and implemented for risk mitigation.
- Regular follow-up on the progress of implementation plans aimed at mitigating risk.

**AUDIT RISK MODEL**

**General**

When conducting audits, the department’s basic scope is to assess the quality of management’s risk management practices within specific operational processes and to provide assurance to the Board of Directors and group management. The auditors devote most of their attention to processes with the highest risk exposures usually the primary activities in the value chain – to ensure maximum added value.

It is clear that internal auditing is a critical factor to efficient risk assessment. The following model of audit risk is useful in planning an audit:

\[ AR = IR \times CR \times DR \]

- **AR** = audit risk
- **IR** = inherent risk
- **CR** = control risk
Audit risk exists for each of the three types of audits which the internal auditor may performs: compliance, operational, and financial.

For a compliance audit, audit risk is the risk perceived from the internal auditor, which he believes that the compliance level is acceptable, when, in fact, it is not. In an operational audit, audit risk is the risk perceived from the internal auditor, which he (who?? it is OK like this, without any other detail??) believes that the levels of operational efficiency and effectiveness are satisfactory, when, actually, they are not. For a financial audit, audit risk is the concluded risk of the internal auditor that misstatements are limited to a tolerable amount, when, in fact, misstatements exceed to the tolerable amount. The tolerable amount is the amount of misstatement which the internal auditor is willing to tolerate without extending the planned audit procedures or giving an unsatisfactory conclusion (Colbert and Alderman, 1995).

**Inherent risk**

Inherent risk is a risk that is intrinsic to the business. The risk of such misstatements is greater for some assertions and balances than for others (Sawyer, 2003). The auditor assesses inherent risk without taking into account the control structure (Gill et al., 2001; Gray and Manson, 2000; Taylor and Glezen, 1991). This means that inherent risk is assessed without taking into account controls which may be in place to prevent non-compliance, inefficient and ineffective operations or material misstatements (Colbert and Alderman, 1995).

The auditor uses his professional judgment and takes into account many factors when assessing inherent risk (Colbert and Alderman, 1995). The auditor is able to assess some of the inherent risk by considering the organization as a whole, because some risks are created by the entity’s culture and management style. Every organization is subject to its own inherent risks and the internal auditor should catalogue them for use in risk assessment. When the auditor assesses the inherent risk, he must establish the obstacles that will prevent from the bad implications resulting from those risks. This consideration deals with the control risk.
Control Risk
Control risk is the risk that non-compliance, inefficient or ineffective operations, are not prevented or detected by an entity’s internal control structure, procedures or policies (Sawyer, 2003). The internal auditor first deal with the control structure and then control risk is assessed. Some control risks will always exist due to inherent limitations of any internal control structure. In other words, since there is no way, risk to be zero, there will be some risks even after the best controls have been installed. That degree of risk is control risk.

If the auditor assesses control risk at its maximum level tests of controls need not be performed. However, if control risk is assessed at a level below the maximum, the auditor identifies policies and procedures that are relevant to the engagement. Then the internal auditor performs tests of controls to support the lower level of control risk (Colbert and Alderman, 1995).

Detection Risk
Detection risk is the risk that the internal auditor does not detect material misstatements, instances of non-compliance, or inefficient or ineffective operations. That is, assuming non-compliance occurs, operations are inefficient or ineffective, or a misstatement enters the system, and the control structure does not prevent or locate the situation, there is a risk that the problem may remain because the auditor does not detect the problem (Colbert and Alderman, 1995).

When audit risk has been established and inherent risk and control risk have been assessed, the internal auditor solves the audit-risk equation for detection risk.

Therefore the equation becomes: \( DR = \frac{AR}{IR} \times CR. \)

An auditor would select those audit procedures that in his crisis would reduce detection risk below the planned detection risk. This emphasizes the concept that inherent and control risk exist independent of the audit. Based on the planned level of detection risk, the auditor adjusts the nature, timing, and extent of substantive testing. On the one hand, if planned detection risk is low – thus, the internal auditor must plan substantive tests to
achieve high confidence - the internal auditor adjusts the nature, timing, and extent of substantive procedures in response to the planned level of detection risk. The auditor may plan substantive tests which provide more reliable evidence or test more items. On the other hand, as planned detection risk rises, which means that the internal auditor receives the required confidence from substantive procedures, he has the ability to reduce them.

To best understand the procedures, we have the ability to observe Table 1, which contains information about total audit risk, its components and the amount of evidence that are required.

**Table 1: Different levels of risk**

<table>
<thead>
<tr>
<th>Cycle</th>
<th>A. e.g Sales</th>
<th>B. e.g Production Cycle</th>
<th>D. e.g. Order Cycle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auditor assessment for the probability to have misstatements without considering the internal control system (inherent risk)</td>
<td>We expect many misstatements (High)</td>
<td>We expect few misstatements (Low)</td>
<td>We expect few misstatements (Low)</td>
</tr>
<tr>
<td>Auditor assessment for the efficiency of internal control system to prevent the misstatements (control risk)</td>
<td>High efficiency of internal control system (Low)</td>
<td>High efficiency of internal control system (Low)</td>
<td>Medium efficiency of internal control system (Medium)</td>
</tr>
<tr>
<td>Quantity of evidence that the auditor aims to collect (detection risk)</td>
<td>Medium (Medium)</td>
<td>Low (High)</td>
<td>Medium (Medium)</td>
</tr>
</tbody>
</table>

From the above table main the outputs are:

- ✓ Inherent and Control risks exist independent of the audit
For a particular level of planned audit risk, inherent risk and control risk are inversely related to detection risk

Detection risk is inversely related to the evidence that must be accumulated

CONCLUSIONS

The last few decades have been characterized by unparalleled change. Nowadays, researchers pay more attention to risk management due to its great importance for the world economy. Simultaneously, all auditing information is established as an essential mean for the exact management of any business economic resources. In today’s highly competitive business environment, internal audit plays a catalytic role (Papastathis, 2003; Papadatou, 2005). As Power (2004) states: “internal control is an unshakeable part of the moral economy of organizations”.

Nowadays, it is a fact that, internal audit has experienced a very hard period but made great progress. During the twenty-first century, internal audit will see its great improvement in many business fields such as risk assessment. History will witness that we will be able to grasp the current favourable opportunity, overcome all difficulties and make new achievements in internal auditing. Internal audit will surely have bright future prospects in business success and especially in efficient risk management.

Last, a possible limitation of the research results is that little work has been undertaken concerning the collaboration between internal audit and risk management in an international context. Thus a suggestion for future research would be to examine the possible applications of internal control system in risk assessment for a longer period with even more studies in a worldwide perception. Another promising research initiative would be to further explore how a risk management system based on the internal control system might be best operationalised to business entity. In this concept, researchers should examine an ex post review to ensure that the risk assessment model that is being used reflects the actual risks faced by an organization. Significant differences should be investigated and the risk assessment model revised to include missing variables.
REFERENCES


Eleftheriadis, I. 2006, “Risk Management Processes. The Case of Greek Companies”, 1st International Conference of Accounting and
Finance, University of Macedonia, Thessaloniki, Greece, Conference Proceedings.


The Institute of Internal Auditors (1999) "Definition of Internal Auditing", The Institute of Internal Auditors, Altamonte Springs, FL.

The Institute of Internal Auditors (2000) "Internal Auditing: Adding Value across the Board, IIA, Corporate Brochure.

