INTERNAL CONTROL SYSTEM AND MANAGEMENT INFORMATION SYSTEMS

Dr. Theofanis Karagiorgos¹, Ioanna Chatzispirou², Dr. George Drogalas³,

Abstract: Rapid changes in information technology and managerial practices in many organizations were forcing efficient internal audit as a tool for reducing the total risk. Simultaneously, information has become one of the most valuable assets of the corporation, and must be protected with care and concern, because business continuity and success are heavily dependent upon the integrity and continued availability of critical information. Within this framework of extremely fluid business environment, the objective of this research is to explore the existence and adequacy of internal control system in management information systems. The results point out that internal auditors pay attention to “traditional” risks that are associated with information systems’ security, while they should take into consideration risks and controls associated with the other units, in order to make information system audit’s function more effective, improving thereby the internal audit’s operation.

Keywords: Internal auditing, Auditing, Internal auditor, Accounting, Management Information System

JEL Classification: M40, M41, M10.

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 Ioanna Chatzispirou: Msc in Management Information System, University of Macedonia, Greece.
³ Dr. George Drogalas: Adjunct Professor, Department of Accounting, Technological Educational Institute of Serres, Greece. Mailing Address: End of Magnisias Str., Serres, Greece Zip Code: GR-540 06, Tel.: 00302321049103, E-mail: georgedrogalas@yahoo.gr
Corresponding Author.
1. INTRODUCTION
To make a rational decision it is essential to use accurate and free of bias information. Specifically, in the context of globalized economy, the need for reliable information on enterprises increases (Konrath, 1996; Power, 2004). In this context, evaluation, control and verification of information performed by a qualified person who will be independent as to the expression of his opinion, is the key for the discovery and use of reliable information (Mihret and Yismaw, 2007).

In other words, internal auditing contributes to the reliability of information that the management uses on the decision-making, in order to ensure that an economic unit operates effectively, deals with risks and achieves its objectives (Roth and Espersen, 2002). Therefore, internal auditing plays important role in the modern business environment (Dittenhofer, 2001). In addition, taking into consideration the entry of complex information systems used for collecting, processing, diffusing information and the implementing of the overall activities’ transaction, it is clear that a complete control system guaranteeing the safety and viability of information systems is needed (Papastathis, 2003).

The effectiveness of internal audit in management information systems is generally a new research area at international level and on a national basis in Greece. Due to the fact that a limited number of studies exist this makes the theme a desirable for research. The purpose of this paper is to investigate the importance of internal auditing, and particularly of information systems auditing in modern business. The self-administered questionnaire that is used for the survey focuses on two points. The research examines, on the one hand, the extent to which internal auditing is carried out in the corporation, on the other hand, the extent to which internal control systems are examined within an information technology (IT) infrastructure.

The structure of this paper is as follows: the next section discusses the conceptual meaning of the term “internal auditing”. Then section two describes the theoretical background of internal auditing and presents the recent literature review. The third section presents the research design by providing information on the development of the survey, the methodology for data analysis and the methodology for the questionnaire. The results of the study are reported and discussed in the fourth section. Finally, the last section contains conclusions, remarks, limitations of the study and recommendations for future research concerning internal auditing and management information systems.

2. LITERATURE REVIEW
2.1 Theoretical Framework of Internal Auditing
Indicative of internal audit’s great importance is the significant amount of definitions that are given by many researchers (Drogalas et al., 2005). In this concept, it is worth mentioning that 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 (Karagiorgos et al., 2009).

More specifically, the Institute of Internal Auditors, (IIA, 1991; Taylor and Glezen, 1991; IIA, 1995) defined internal auditing as “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, becomes 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).

Hence, the U.S. Government Accountability Office noted that internal auditing is “an integral component of an organization’s management that provides reasonable assurance that the
following objectives are being achieved: effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations” (GAO, 1999).

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). 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).

A more specific definition is given by Sawyer (2003) who stated that internal auditing is “a systematic, objective appraisal by internal auditors of the diverse operations and controls within an organization to determine whether (1) financial and operating information is accurate and reliable, (2) risks to the enterprise are identified and minimized, (3) external regulations and acceptable internal policies and procedures are followed, (4) satisfactory operating criteria are met, (5) resources are used efficiently and economically and (6) the organization’s objectives are effectively achieved – all for the purpose of consulting with management and for assisting members of the organization in the effective discharge of their governance responsibilities”(Karagiorgos et al., 2009).

From the above definitions, it is clear that the internal control is not just an one-sided tool for controlling the order and rightness of certain situations, but it is a method of detecting the value added up to a company, achieving the index of effectiveness and profitability of the company (Nagy and Cenker, 2002; Goodwin, 2004; Zain et al., 2006)).

2.2 Recent Empirical literature
The critical role of computers in modern business prompts enterprises to take special measures in order to protect their information systems and ensure their accurate and safe function. The combination of automated and non-automated procedures with the aim to protect information systems is called auditing. Information systems audit includes the methods, the policies and the procedures that provide information assurance and security, assets safeguard, data integrity maintenance, and compliance with law and regulations. Moreover, these procedures manage to mitigate risks concerned with the use of information technology by organizations, and to minimize the damage caused from computer errors, electronic crime and security breaches.

In 1998, Rezaee and Reinstein studied the impact of informational technology on auditing activities. Their study was centered on the key issues of SAS No. 80 that offer auditors guidance to obtain sufficient evidence so that they evaluate their clients’ information systems. Rezaee and Reinsein (1998) argued that information technology contributed to the simplification of information entry into the transactions and the overall processes. Also, according to Rezaee and Reinsein, due to information technology, the evaluation of the related controls and results became more critical. To accumulate sufficient evidence and therefore make informed decisions, answers must be given to certain questions, such as where to look for that evidence, what auditing processes to take into consideration and how to evaluate these processes.

Through the report published in 2000, the Public Oversight Board expressed concerns about the ability of auditors to properly assess the risks arising from rapid changes in information systems. The POB encouraged auditors to expand their knowledge of information systems, hoping to help themselves with the development of more effective audit approaches. Furthermore, the POB recognized the need to attract and keep qualified technical IT specialists for the audit function and confirmed that more and more auditors would find out that it is necessary to fully understand the risks associated with new and advanced information systems as well as the controls that are needed to address those risks.
Hermanson et al. (2002) conducted a survey to examine internal auditors’ activities related to information technology, in U.S.A. companies. The evidence gathered from more than 100 directors of internal auditing showed that internal auditors focus primarily on “traditional” risks and audits, such as safeguarding of IT asset, data integrity and security, while giving little attention to other risks such as those related to systems development and acquisition. According to the results, many factors affect the internal auditors’ performance of IT evaluation, including the nature of the audit target, the prevalence of specific information systems audit specialists on the internal audit staff and the availability of new information systems.

In 2003, Rishel and Ivancevich, claimed that the basic responsibilities of internal auditors had to do with risk management issues and control especially during the pre-implementation and monitoring phases of informational technology projects. Through their study, they argued that internal auditors should pay attention to system configuration and IT implementations to ensure that adequate controls are performed. Additionally, internal auditors should communicate with the IT department to assure that not only new systems but also modifications to existing systems are well documented, as proper documentation is essential to internal audit in terms of evaluation of risks and controls.

In the same period, Meredith and Akers (2003) conducted a survey to investigate whether consulting affects the independence of the internal audit function. They surveyed 241 chief executive officers (CEOs) and examined their opinions on internal audit’s involvement in systems development, and particularly they examined whether such involvement sets in danger the independence of internal auditors and if auditors should act as consultants for systems development projects. The results revealed that what interests CEOs more is the maintenance of internal audit function’s independence even if the internal auditors act as consultants. Respondents were unconcerned about internal audit’s involvement in the planning and design phases and did not support its involvement in the development, implementation and maintenance phases. The results of the comparison of perceptions between CEOs and chief audit executives (CAEs) revealed that there are significant differences between these two categories regarding their expectations. CEOs considered independence to be the most important matter, while CAEs emphasized the need for internal auditors to act as consultants.

In 2003, Hadden et al. investigated the IT qualifications and activities of audit committees, internal and external auditors with regard to IT risk management. The results of the study suggested that audit committees appear to offer limited supervision of IT-related risks, while they do believe that they should take a more active role in this field. As for internal auditors, the results revealed that their involvement in information technology oversight was rated as “above average”, while the respective involvement of the external auditors was rated as “moderate”.

One year later, Hunton et al. (2004) carried out a research in order to examine, understand and assess the extent to which financial auditors and information systems auditors are able to identify the audit risks associated with ERP systems. The results revealed that financial auditors are less interested in ERP risks compared to information systems audit specialists, while the second ones dispute financial auditors’ ability to identify risks associated with ERP systems, something which could have negative effects on audit quality.

The threats of computerized accounting information systems (CAIS) in Saudi companies were examined by Abu-Musa (2006). The results revealed that nearly half of the responding Saudi companies suffered financial losses due to internal and external security breaches of CAIS. Moreover, the most significant security threats to CAIS in Saudi companies were highlighted. These are accidental or intentional entry of false and invalid data, accidental data destruction...
by employees, disclosure of employees’ passwords, introduction of viruses to CAIS, destruction of output, unauthorized viewing of documents as well as the distribution of information to unauthorized individuals. The study presents some recommendations to strengthen the security controls of information technology and to enhance the awareness of CAIS security issues in Saudi companies in order to manage the IT risks more efficiently and ultimately to protect their CAIS.

In 2006, Bierstaker et al. conducted a survey to assess the extent to which methods of detecting and preventing fraud are being used. For this reason, 86 accountants, internal auditors and certified investigators against the fraud were surveyed about the effectiveness of those methods. The results revealed that the most common methods and measures to deter fraud are firewalls, anti-virus protection, protection of passwords and review as well as improvement of internal control.

Finally, the research carried out by Abu-Musa, in 2008, aimed to examine both the impact of the emerging information technology in internal auditors’ activities and the extent to which the IT assessments held in Saudi firms vary based on evaluation objectives and organizational characteristics. The results revealed that internal auditors should enhance their knowledge and qualifications related to information systems (CIS) for the design, administration, supervision and review of the work performed. Moreover, the results are consistent with those of the Hermanson et al. study in that the internal auditors focus mainly on “traditional” risks and controls, such as integrity of data, privacy and security, safeguarding of assets and processing applications. It was also found that less attention is given to system development and acquisition activities. The informational technology evaluation performed by internal auditors is connected with many factors, such as the audit objectives, the type of operation, the number of the information system auditors in the audit staff as well as the existence of new information systems.

**RESEARCH DESIGN**

To describe more realistically the importance of internal audit in the management information systems, the sample of research was companies listed on the Greek Stock Exchange. To achieve its goal the research uses the exploratory research methods of research questionnaires. To enhance the survey response rate preliminary contact was made with potential respondents ahead of sending the questionnaire. Cover letters and surveys, along with postage paid return envelopes, were mailed directly to each of the business executives. Hence, correspondence was personalized as far as possible; cover letters were hand signed; and envelopes were individually addressed with the name and title of the business executive. However it should be mentioned that even the organizations, which finally completed the questionnaire, initially were not willing to complete it, because they believed that data about the security of their information systems should not be disclosed outside their organizations. They finally agreed to complete the questionnaire after we signed a non-disclosure agreement.

The questionnaire used for the survey included multiple choice questions and questions for the measuring of variables using the five-point Likert scale, where the respondent is requested to rate a series of clauses regarding internal audit and information systems auditing, stating the degree of agreement or disagreement. The questionnaire is designed in such a way that enables its rapid completion. For this reason, it is separated into four main parts:

1) Part A refers to the general internal audit’s evaluation.
2) Part B refers to information systems auditing and how that is implemented in each thematic area.
3) Part C refers to the usage of computer assisted audit techniques (CAATs).

Respondents were asked to indicate their degree of agreement or disagreement with each of the statements on a five-point Likert response scale that ranged from “strongly agree (scored
as 5) to “strongly disagree” (scored as -1). This methodology was employed because it is relatively easy for respondents to use, and responses from such a scale are likely to be reliable.

4. RESULTS
About 204 questionnaires were distributed to different organizations. After excluding incomplete and invalid questionnaires, the research ended with 38 valid and usable questionnaires representing a 18.6 percent response rate. More specifically, six of the respondents were Merchandising companies (15.8 percent), five of the respondents belonged to the branch of Industrial Products (13.2 percent), five respondents belonged to the branch of Raw Materials (13.2 percent), four respondents were from the Banking Sector (10.5 percent), four respondents belonged to the Domestic branch (10.5 percent), four respondents were from the Food Industry (10.5 percent), three respondents were Manufacturing companies (7.9 percent), three respondents were from the Chemical Industry (7.9 percent), two respondents were from the Health Sector (5.3 percent), one respondent was from the Hotel Industry (2.6 percent) and one respondent belonged to the Insurance Industry (2.6 percent). Regarding the status of the respondents and their position in the company, 16 of them were Internal auditors (42.1 percent), 10 of the respondents were IT/IS Directors/ Auditors (26.3 percent), two respondents were Information Technology Managers (5.3 percent), one respondent was Director of Finance & Chief Accounting (2.6 percent), one respondent was Head of Technical Department (2.6 percent), one respondent was Human Resources Manager (2.6 percent), while the remaining seven respondents (18.5 percent) gave no answer.

Part A of the questionnaire refers to the internal audit’s general organization and operation. Question 1 examines the person who is responsible for the performance of information systems evaluation. The 39.5 percent of the respondents replied that experts of IT department are responsible for information systems evaluation, while an equal percentage answered that internal auditors are in charge of this activity. The remaining eight companies responded that information systems evaluation is performed either by internal and external auditors (five replies), or exclusively by external auditors (3 replies). The second question examines to whom internal audit reports. The majority of the respondents (47.4 percent of the total responses) answered that internal audit reports to the Audit Committee. A rate of 23.7 percent of the respondents answered that internal audit reports to the Board of Directors, while 18.4 percent of the respondents answered that internal audit reports to the President of the Board. Additionally, two of the respondents answered that internal audit reports both to the Board of Directors and the Audit Committee, while the rest did not give a certain answer. Question 3 investigates whether standards of editorial audit documents exist. According to the results, 86.1 percent of the respondents replied in the affirmative, while only 13.9 percent of the respondents answered negatively or replied that such standards do not exist. The last question examines whether the existing staff meets the needs of internal audit. The vast majority responded positively, while only 18.8 percent of the respondents gave a negative answer.

Part B of the questionnaire deals with matters related exclusively to information systems auditing and evaluation. More specifically, Section B1 refers to IT organization and administration. In question 5, which examines the existence of approved information strategy 39.5 percent of the respondents answered that there is “to a large degree”, 34.2 percent of respondents answered that there is but “on a medium scale”, and even fewer were those who replied that there is “to a very large extent” (21.1 percent). Finally, only 5.3 percent of the respondents believe that such strategy exists to a small degree, while there was no negative response. The next question examines whether risk strategies are followed. The majority responded that such strategies are adapted to a large extent (44.7 percent), 31.6 percent of the respondents answered “to a modest scale”, 18.4 percent answered “to a very large degree” and finally only 5.3 percent answered “to a small degree”. Again there was no negative response. Question 7 examines whether a reporting system of IT Directorate’s responsibilities...
towards the Board has been legislated. The majority of the respondents answered “to a large degree” (36.8 percent). About 23.7 percent of the respondents answered “on a medium scale” and an equal percentage answered “to a large extent”. Even fewer were those who answered that such a reporting system has been legislated, but “to a small degree”, while 5.3 percent of the respondents answered negatively. Question 8 examines whether the procedures related to the supply management and IT budget are properly organized. Obviously, the organization of such procedures is an important issue for most of the businesses, as 39.5 percent of the respondents answered “To a very large extent” and an equal percentage of the respondents answered “on a large scale”. Fewer were those who claim that, this is happening “to a medium degree” (15.8 percent) or even “to a small degree” (5.3 percent).

Section B2 refers to information system development and maintenance. Question 9 examines whether and to what extent companies comply with standards related to the activities of the information systems turnover. Most of the respondents, (44.7 percent) answered “to a large degree”. The next lowest percentage (31.6%) is of those who responded “to a very large degree”. Fewer were those who answered “on a medium scale” (18.4 percent), while only 5.3 percent of the respondents answered “in a small degree”. The next question examines whether and to what extent members of all administrative levels participate in the feasibility study. According to 47.4 percent of the responses members of all administrative levels participate in the feasibility study to a large degree. About 26.3 percent claimed that this participation exists to a medium degree, while 18.4 percent of the respondents answered “on a small scale”, and the rest answered “to a very large degree” (7.9 percent). Question 11 examines whether it is ensured that the changes resulting from the description of all the reports and the new system meet with the management’s approval. The majority of the respondents agreed that this happens to a large degree (52.8 percent), 25 percent replied “to a very large extent”, 16.7 percent of the respondents answered “on medium scale” and only 5.6 percent answered “on small scale”. The last question considers whether the test of acceptance is implemented. The results seem to be similar with those of the previous question, as it is noticed that 44.7 percent and 28.9 percent of the respondents answered “on large scale” and “to very large degree” respectively. A rate of 18.4 percent answered that the acceptance testing is implemented on medium scale, while 7.9 percent claimed that this procedure is followed on a small scale.

Section B3 involves topics related to information system operation and support. Question 13 examines the existence and maintenance of documentation record, so that the protection of organization’s information assets is ensured. The results do not vary that much from those we had previously. About 42.1 percent responded “to a large extent”, and the answers that follow are “to very large degree”, “on a medium scale” and “on a small scale”, gaining 31.6 percent, 21.1 percent and 5.3 percent of the respondents respectively. The next question examines the extent to which documented and integrated facility tests are implemented. A rate of 44.7 percent claimed that such tests take place “on a large scale”, 32 percent of the respondents answered “to a very large degree”, while the 21.1 percent of the total respondents answered “on a medium and small scale”. Question 15 refers to user training and examines to what extent this training is implemented and followed by practical training in simulated environment. “On a large scale” is the most prevalent answer (52.6 percent), while 23.7 percent of the respondents answered “to a very large degree”, 10.5 percent of the respondents answered “on a medium scale” and 7.9 percent of the respondents answered “on a small scale”. It is worth noting that a rate of 5.3 percent claimed that there is no users’ training. Question 16 is concerned with systems support, examining whether and to what extent an overview of the system after the first year of its operation takes place. Half of the respondents answered that this happens on a large scale, while 28.9 percent of the respondents answered “on a medium scale”. Only 13.2 percent responded “to a very large degree”, and just 7.9 percent answered “on a small scale”.

Section B4 includes questions related to IT security. Question 17 examines whether procedures for the access of authorized personnel are documented. A rate of 39.5 percent
responded “to a large degree”, 28.9 percent of the respondents answered “on a medium scale”, 7.9 percent of the respondents answered “to a small extent” while a rate of 5.3 percent claimed that such procedures are not documented at all. Question 18 considers the use of digital signatures, encryption techniques and other procedures, which are useful for the safety of data transmission. Most of the respondents claimed that such procedures are followed to a large and very large extent (34.2 percent and 26.3 percent respectively). However, the number of the respondents who answered “on a medium scale” or “on a small scale” is not negligible quantity (15.8 percent and 13.2 percent respectively). It is worth noting that in this question, a high percentage of the respondents (10.5 percent) chose to answer “Never”. Consequently, there is an urgent to put special emphasis on security procedures and how to improve them, as security is one of the most important issues of risk management. Another very important question regarding safety is question 19 examining the adoption of password handling policies. Exactly half of the respondents answered that such policies are adopted “on a large scale”, and 31.6 percent of the respondents answered “to a very large degree”. A rate of 13.2 percent of the respondents answered “on a medium scale”, and only 5.3 percent answered “on a small scale”. The last question of this section examines the usage of firewalls to prevent access by unauthorized users. It is observed that more than half of the respondents answered “On a very large scale” (52.6 percent) and a rate of 36.8 percent stated that firewalls are used “to a great degree”. The percentage of the respondents who replied that there is medium or little usage of firewalls was up to 5.3 percent in both cases.

Section B5 consists of questions related to contingency and disaster recovery. More specifically, question 21 examines the extent to which mechanisms used for preventing unauthorized access, destruction due to natural causes or shut-down problems, are applied and controlled. It is observed that, a high rate of 60.5 percent responded that such security mechanisms are applied “to a large extent”. Eight of the respondents, representing 21.1 percent of the total responses, answered “to a very large extent”, while 10.5 percent stated that this happens “on a medium scale” and 7.9 percent answered “on a small scale”. Question 22 examines whether and to what extent systems undergo recovery, security and system endurance tests. A rate of 48.6 percent of the respondents stated that such integrated tests are carried out “on a large scale”, 27 percent answered “on a medium scale”, 13.5 percent answered “to a very large extent” and 10.8 percent of the respondents answered “on a small scale”. Again, there was no negative answer. Question 23 examines the extent to which backup procedures are followed. The results showed that keeping backups is a dominant concern of enterprises, as 30 respondents representing 78 percent of the total responses answered that such procedures are followed “to a very large degree”. The percentage of the respondents claiming that such procedures are followed “on a large or medium scale” was up to 10.5 percent in both cases. The last question of Part B of the questionnaire examines the extent to which risk analysis for different categories of issues is performed. The majority of respondents (57.9 percent) answered that risk analysis is performed “on a large scale”, 18.4 percent of the respondents answered “on a medium scale”, 15.8 percent of the respondents answered “to a very large degree”, 7.9 percent of the respondents answered “on a small scale”, while there was no negative response.

Part C of the questionnaire refers to computer assisted audit techniques (CAATs) that are used in information systems auditing. Question 25 examines whether and to what extent the test deck technique is used. This technique includes tests in order to confirm that the system operates properly and information is processing in accordance with the appropriate controls. The results showed that 44.4 percent of the respondents uses this technique “on a large scale”, and 30.6 percent “on a medium scale”. Five of the respondents representing 13.9 percent of the total respondents answered that the above technique is used “to a very large degree”, and four respondents (11.1 percent), stated “on a small scale”. It is worth noting that two of the respondents gave no answer. The next question refers to the usage of integrated test facility technique. This technique involves the continuous and parallel processing of integrated tests with the normal operation of the production system in order to test the information system’s
performance. It was observed that this technique is not used as much as its predecessor, as 37.1 percent of the respondents answered “on a medium scale”, 25.7 percent of the respondents answered “on a large scale”, 20 percent of the respondents answered “to a very large degree”, 11.4 percent of the respondents answered “on a small scale”, while a rate of 5.7 percent responded that it is not used at all. It is worth noting that three of respondents ignored the question. The next technique to be considered is that of the parallel simulation. Using this technique, IT operating processes are simulated and the test results are compared to the results of the production information system. The number of the respondents who answered “never”, “on a small scale” and “on a large scale” does not differ from those of the previous question. The number of those who answered that this technique is used “on a medium scale” was increased (45.7 percent), while only four of the respondents, representing 11.4 percent of the total responses, claimed that the technique of parallel simulation is used “to a very large degree”. Three of the respondents gave no answer. Another technique that belongs to the CAATs is the audit file triggering technique. This technique is used for the activation of audit files in which all the transactions during specific controls over data processing are recorded. A rate of 37.1 percent answered that this technique is used “on a medium scale”, while a slightly lower percentage of the respondents (31.4 percent) answered that it is used “to a large degree”. A rate of 20 percent answered “on a small scale”, 8.6 percent of the respondents answered “to a very large degree” while only one respondent said that this technique is not used at all. It was also observed that tree of the respondents gave no answer. Question 29 refers to program checking technique. This technique analyses the program code and records all the transactions and the logical interfaces for control purposes using the audit software. The results showed that this technique is used “to a large degree” according to a rate of 42.9 percent of the respondents, and “on a medium scale” according to a rate of 28.6 percent of the respondents. Six of the respondents, representing 17.1 percent of the total responses, answered “to a very large degree”, and three of them (8.6 percent of the respondents) answered “on a small scale” while there was one respondent who answered that the technique is not used at all. Three of the respondents preferred to give no answer. The last discussed technique is that of the mapping of processing technique. This technique is used for the documentation of the logical interfaces, which have not been tested, and it is also used for the control through test movements as well as the comparison of the results with those expected. A rate of 37.1 percent answered that this technique is used “on a medium scale”, 22.9 percent of the respondents answered “to a very large degree”, 17.1 percent of the respondents answered “on a large scale”, 14.3 percent of the respondents answered “on a small scale” and a rate of 8.6 percent claimed that this technique is not used at all. Three of the respondents did not answer.

5. CONCLUSIONS
Effective control over all business activities, prevention of potential fraud, avoidance of failures, effective business risk assessment, enhancement of the company’s transparency and role in the economic domain, achievement of a company’s goals are some of the undeniable benefits of the independent internal audit function (Asairy, 1993; Cangemi and Singleton, 2003). Internal auditing is not limited to the traditional financial audit, but offers its consulting services in a wider range of functions and activities (Kantzos and Chondraki, 2006). Thus, one of the main types of internal audit is the information systems auditing, which is a process of evaluating evidence of an organization’s information systems so as to determine whether these systems are safeguarding assets, maintaining data integrity, operating effectively to achieve the organization’s objectives and the efficient consumption of resources (Yang and Guan 2004). The role of information systems auditors is critical, as they enhance information technology governance, assess risks and implement controls over those risks (Rezaee et al., 2001). An effective information systems audit function should be centred on the risks arising from information systems development, implementation and operation. Such a function should examine the adequacy of internal controls and recommend where necessary appropriate modifications. Hence, such a function is supposed to measure the compliance with the operational strategy and the entity’s documented policies, standards and
procedures. A comprehensive view of the information systems operation is essential in order to keep the audit committee adequately informed on a regular basis.

The above approach was the basis of the current research. Taking into account suggested methodologies for conducting informational technology audits as well as other questionnaires, the present questionnaire was designed aiming through a structured and detailed set of general principles and criteria to give a comprehensive picture to the readers of the evaluation of the operational efficacy and security that is subject to information systems auditing. These principles are grouped into five sections, which are IT Organization and Administration, Information System Development and Maintenance, Information System Operation and Support, IT Security, Contingency Planning and Disaster Recovery. Moreover, the questionnaire included general questions related to internal controls evaluation as well as questions regarding computer assisted audit techniques. Using the Likert scale some conclusions are drawn from the statistical analysis of the results.

Beginning with the general questions of Part A of the questionnaire, we note that there is no prevalent answer regarding the responsible person that is designated by the entity for the information system audit. The answers are shared among the IT department and the Internal Auditor. A rate of 45.9 percent answered to question 2, that internal audit reports to the Audit Committee. Finally, the vast majority responded positively to questions 2 and 3, confirming that standards of editorial audit documents do exist (86.1 percent of the respondents), and the existing personnel does meet the needs of the department of internal controls (81.25 percent of the respondents).

The statistical analysis of Part B of the questionnaire shows that the responses given are in principle positive, indicating however that further improvement can be achieved. Thus, regarding B1 section, we find out that companies do not pay enough attention to issues related to IT Organization and Administration. This conclusion draws from the fact that more than half of the respondents agreed that there is registered and approved strategy which is in harmony with organization’s objectives, that procedures related to the supply management and IT budget are properly organized and that IT Directorate reports to the Board. However, many were the respondents who argued that the above stand on a medium or small scale, representing a not insignificant proportion of 40 percent of the responses. The results of B2 section seem to be more satisfactory as most of the respondents agreed that companies comply with standards related to the activities of the information systems turnover, all the required changes are approved by the Board and the test of acceptance of a new system is implemented. In the question concerning the participation of members of all administrative levels in the feasibility study, the answers seem to be more cautious as a proportion of 44.74 percent claimed that this happens on a small or medium scale. The analysis of the responses at B3 section shows that companies adopt practices that ensure the operational continuity and effective support of information systems. The majority of the respondents confirmed that a documentation record does exist, training of users is held and also overview of the system after the first year of its operation takes place. Observing the results of the responses at B4 section, we find out that the majority of the respondents confirmed that companies focus on the adoption of password handling policies (81.58 percent answered “on a large and very large scale”) as well as on the usage of firewall (89.47 percent answered “to a large and very large extent”) and consider such mechanisms to be the best practices and security measures of their information systems. There is urgent to put more emphasis on documented procedures regarding the access of authorized personnel as well as on security procedures for data transmission, as such procedures seem to be missing. All of the above special measures are necessary to companies, especially in case those companies are engaged in e-commerce and digital business processes. The responses at the last section of the questionnaire were positive and thus satisfactory in the main. It is worth noting that approximately 80 percent of the companies are concerned with backup procedures, preventive or measures taken for disaster recovery, based on the results.
The analysis of the responses at Part C of the questionnaire shows that computer assisted audit techniques are not used to a large extent. The most common technique is that of program checking and the least common technique is that of audit file triggering. The results are rather disappointing and that is due to the fact that companies are probably unaware of such techniques, the use of which may contribute to better control and verification of the information systems’ validation checked by the auditors.

In conclusion, we could claim that this study contributes to the literature by providing empirical results on the relationship between internal audit and management information systems. The main output is that auditors pay attention to “traditional” risks that are associated with information systems’ security and also to contingency planning, while they should take into consideration risks and controls associated with the other units too, in order to make information system audit’s function more effective, improving thereby the internal audit’s operation. However, as with other studies, the findings of this study should be viewed taking into account its limitations. The sampling area of the study was limited to the companies listed on the Greek Stock Exchange. Hence, 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 further limitation in carrying out this study, to be taken into account particularly if one is to compare these results to those that may be found in other countries, is the small number of respondents on which the study was necessarily based.

Concluding, this research did not have the intention of concluding the discussions over the interaction between internal audit and management information system; however, it is expected to be one more element to help the formation of opinions and to diffuse other discussions on the subject. Further research could be conducted on an industry basis to generate comparative findings on the existence of internal auditing and the extent to which information systems auditing takes place, that is something which requires much more time as well as the organizations’ willingness to participate in such research. Furthermore, it is recommended further research by examining the matters reported in this paper via different methodologies. Finally, it is recommended to carry out some future research to collect further empirical evidence by doing selected interviews or conducting some cases studies in order to gain more in depth and congruent empirical results that may be crucial for new practical recommendations for the Greece business sector.
REFERENCES


