Internal auditing and cyber security: audit role and procedural contribution

Petros Lois*

Department of Accounting,
School of Business,
University of Nicosia,
Makedonitissis 46, 2417, Nicosia, Cyprus
Email: lois.p@unic.ac.cy
*Corresponding author

George Drogalas

Department of Business Administration,
University of Macedonia,
156 Egnatia Street, GR 54636, Greece
Email: drogalas@uom.gr

Alkiviadis Karagiorgos

Department of Accounting,
School of Business,
University of Nicosia,
2417, Cyprus
Email: alkiskar@gmail.com

Alkis Thrassou and Demetris Vrontis

Department of Marketing,
School of Business,
University of Nicosia,
Makedonitissis 46, 2417, Nicosia, Cyprus
Email: thrassou.a@unic.ac.cy
Email: vrontis.d@unic.ac.cy

Abstract: Businesses operate in a dynamic environment that is constantly changing and in which they are undermined by various risks. One in particular, is that of cyber security. Internal auditors, through their multifaceted role, can contribute to the reduction of the information systems' violation. Extant works, nevertheless, on the connection between internal audit and cyber security worldwide, are scant, and practically non-existent for the case of Greece. Thus, the purpose of this paper is to examine the variables that influence cyber security and which, at the same time, are relevant to internal audit. In this context, methodologically, a questionnaire was distributed to companies listed

on the Athens Stock Exchange and addressed to their internal auditors. The findings of the survey identified key factors impacting cyber security, including the degree and nature of cooperation between IT staff and auditors, and training regarding information technology.

Keywords: cyber security; internal audit; factors; service.

Reference to this paper should be made as follows: Lois, P., Drogalas, G., Karagiorgos, A., Thrassou, A. and Vrontis, D. (2021) 'Internal auditing and cyber security: audit role and procedural contribution', *Int. J. Managerial and Financial Accounting*, Vol. 13, No. 1, pp.25–47.

Biographical notes: Petros Lois holds an MSc in Accounting and PhD degree (UK). He is a Certified Management Accountant-CMA and holds the Chair of PwC in Business Research at the University of Nicosia. He is currently the Head of the Department of Accounting, and Director of a joint Master in Banking, Accounting and Finance. He is a member of the Institute of Certified Management Accountants of Australia-ICMA, and the Institute of Marine Engineers, Science and Technology-IMarEST, UK. He served as a member of the Board of Directors of the Cyprus Ports Authority-CPA. His research interests include accounting, auditing, working capital management, and finance. His research work has been published in international conference proceedings, books and journals.

George Drogalas is currently an Assistant Professor in Accounting at the Department of Business Administration (University of Macedonia). He received his Bachelor degree from the Department of Business Administration (University of Macedonia), an MBA degree in Accounting and Auditing from the Department of Business Administration (University of the Aegean) and a PhD degree in Accounting and Auditing from the Department of Business Administration (University of Macedonia). He worked as a Chief Internal Auditor. His research focus is on auditing, internal audit, managerial accounting, audit committees and IFRS. Finally, he is a Certified Internal Controls Auditor (CICA).

Alkiviadis Karagiorgos received his PhD from Business Administration Department, at Piraeus University. His research aims at intangible assets costs, knowledge capital and cost accounting systems development. He is the co-owner and Chief Editor of Karagiorgos Bros SA Accounting and Publishing. He served as the Secretary of the Doctoral and Postgraduate Students Association at the University of Macedonia and later representative of doctoral students to the General Assembly for the Department of Business Administration at Piraeus University. He is an instructor at the University of Nicosia, International Hellenic University, and the University of Macedonia. His work is published in international conferences, books and journals.

Alkis Thrassou is a Professor at the School of Business, University of Nicosia (Cyprus,EU). He holds a PhD in Strategic Marketing Management from the University of Leeds (UK), as well as a BEng (LU) and an MSc (UNIC) in Engineering. He is also a Chartered Marketer and Fellow (FCIM), a Chartered Construction Manager and Fellow (FCIOB), a Chartered Management Consultancy Surveyor (MRICS), and a Senior Research Fellow of the EuroMed Academy of Business (SFEMAB/EMRBI). He is an Associate Editor of the *EuroMed Journal of Business* (Scopus cite-score 5.1) and Managing Editor of the *Palgrave Studies in Cross-disciplinary Business Research*. He has extensive academic and professional/industry experience, and he has undertaken significant research in the fields of management and strategic marketing. He

has published over 180 works in numerous internationally esteemed scientific journals, books and conferences; edited/guest-edited numerous journals and books; and retains strong ties with industry, acting also as a consultant.

Demetris Vrontis is the Vice Rector for Faculty and Research and a Professor of Strategic Marketing Management at the University of Nicosia, Cyprus. He is the Founder and Editor-in-Chief of the *EuroMed Journal of Business*, an Associate Editor of the *International Marketing Review* and an Associate Editor of the *Journal of Business Research*. He is the President of the EuroMed Academy of Business and the Managing Director of Gnosis: Mediterranean Institute for Management Science. He has widely published in about 300 refereed journal articles, 45 books and 60 chapters in books, and has presented papers to over 80 conferences around the globe. He is a fellow member and Certified Chartered Marketer of the Chartered Institute of Marketing and a Chartered Business Consultant.

1 Introduction – research context

In recent years, the way businesses operate has changed, corresponding to continuous changes arising at economic, technological and other levels that make it imperative for services to apply internal audits (Drogalas et al., 2015; Siouziou et al., 2017). Increasing market competitiveness levels urge companies to explore new methods towards competitive advantage and survival. Today, stakeholders, if versed in their respective fields and capable of applying specialised knowledge, could be part of a company's possible strategies for improved performance (Caputo et al., 2018) and information can facilitate such processes and management efforts through proper communication strategies. Thusly, stakeholders' knowledge and successful information sharing policies can develop swift and competitive strategies (Giacomarra et al., 2019; Fjellström et al.. 2020). In an uncertain environment, businesses must respond to incurred risks with the contribution of internal audit being crucial (Drogalas et al., 2016, 2015).

One grave and modern risk is cyber security assurance, which stems from the digitisation that has taken place in recent years through the implementation of information systems. However, the use of these systems can have adverse consequences in cases of cyber violation (Da Veiga and Eloff, 2007; Yeboah-Ofori and Islam, 2019). Furthermore, these violations are becoming more frequent, resulting in significant losses (Clark and Harrell, 2013), making it vital for organisations to respond to this issue, also by efficiently exploiting diverse cross-functional innovation strategies for planning and implementation of operations (Shams et al., 2018). In this vein, internal audit, whose role has expanded due to modern changes, must actively contribute to safeguarding security of online services and processes (Sarens and De Beelde, 2006; Abu-Musa, 2008).

The ever-increasing incidents of breaches in business information systems have drawn the attention of businesses to the methods needed in order to limit these incidents and their effects (Gordon et al., 2003). The fiscal crisis of 2009 has also reinforced abusive behaviours (Broom, 2009), and although complete eradication is considered unfeasible, it can be managed if protective measures are implemented properly (Kahyaoglu and Caliyurt, 2018). However, the methods proposed by information technology (IT) experts are not sufficient. In order to ensure the security of information

systems containing sensitive information, it is necessary for internal audit to contribute towards the same protection goals (Eling and Schnell, 2016; Steinbart et al., 2018).

Fielden (2011) proposed a holistic framework for information security, including social and technological factors. Technological advances are indispensable for the establishment of an effective digital auditing system (Lois et al., 2019a). Clark and Harrell (2013) focused on the contribution of business boards to security, arguing that business should invest in security. On the other hand, the latter investigated the contribution of internal audits to risk management and corporate governance by comparing the US and Belgian firms. In addition, Thompson (1998) dealt with cybercrime in Australia, focusing on cyber threats and on the contribution of state law enforcement agencies to security. Despite the positive impact that internal audits can have on security of online services, few researches have approached this technological issue (Steinbart et al., 2018). Furthermore, security of online services has also been studied by many IT experts, but there is an evident lack of studies at the managerial level (Eling and Schnell, 2016). The purpose of this article is to examine the factors that affect the security of electronic processes related to internal audit.

In this light, there is a growing interest in conducting both theoretical and empirical research in Greece on the factors related to internal audit and that affect the security of information systems in order to enrich international literature and the role of internal audit. The paper is structured first by arguing the necessity for a theoretical framework in Section 2. The theoretical foundation and hypothesis presented in Section 3, followed by the research methodology in Section 4 and the Results in Section 5. The article discusses and concludes with the main conclusions comparing the results of the present study with other research and suggestions for future research in Section 6 and Section 7, respectively.

2 The need for a theoretical framework

Businesses are making changes to keep up with new developments and pursue added value activities implementations (Chebbi et al., 2013). At this point, internal audit is necessary as it will act as an advisory body to management and provide information needed for decision-making (Bou-Raad, 2000). Internal audit is now an integral part of business (Dittenhofer, 2001; Drogalas et al., 2016; Siouziou et al., 2017). The role of internal audit is to operate independently, control the achievement of objectives and contribute to the proper performance of its functions (Drogalas et al., 2015). In particular, internal audit takes into account corporate governance and assists risk management, with the aim of achieving effective business performance through advice, suggestions and controls (Cohen and Sayag, 2010; Drogalas et al., 2015). Part of internal audit is also to safeguard the businesses' compliance with rules and laws that govern its operation, as well as to ensure business integrity (Dittenhofer, 2001). By checking the proper functioning, internal audit can identify various omissions and potential risks, thus taking the necessary steps to avoid adverse events. However, internal audit is effective when it ensures its independence from management, when there is professional training of executives, and when it fulfils the goals of stakeholders (Cohen and Sayag, 2010). Moreover, audit efficiency is influenced by the low or high strength rate of audit reporting standards depending on audit's importance for each country (Khlif and Guidara, 2018). Proper functioning of internal audit can aid in the reduction of infringements

and fraud, as well as in ensuring the integrity and security of information and its transmissibility (Siouziou et al., 2017).

The rapid development of technology and the increasing usage of new technologies create the need for protection against malicious activities that target information systems (Gordon et al., 2003; Hannaford, 1995). The security of electronic services concerns cyber security between networks (Eling and Schnell, 2016; Zakaria et al., 2019). A key concern of businesses is to have information systems that do not allow unauthorised users access and ensure that information is not vulnerable to spying or other incidents of infringement (Gordon et al., 2003). Cebula and Young (2010) defined online risks as operational risks in information and technology elements, which have implications for the confidentiality, availability or integrity of information or information systems. These issues in a lesser degree are also obvious in public sector audits, where protection against cyber attacks is deemed to become of grave importance in the near future (Alali et al., 2018; Lois et al., 2019b).

Security should be integrated into software as well as operating systems, as information systems themselves must reach the desired level of security. In addition, emphasis should be placed on network security through which business employees communicate with each other, but also at an administrative level, as there should be a unified security policy that avoids and poses potential risks (Hannaford, 1995).

Businesses are now faced with new risks, such as the attacks taking place in the digital world (Trim and Lee, 2010; Hannaford, 1995; Souppaya and Scarfone, 2013; Kahyaoglu and Caliyurt, 2018), which may cause serious negative consequences for businesses, such as loss of credibility or clients, leading to financial deficiencies (Eling and Schnell, 2016). The effectiveness of electronic processes and systems security, based on Steinbart et al. (2015, 2018), can be measured by the number of violation incidents in the previous year, the trend of these incidents in the last three years, and the number of incidents detected and handled before they have a negative impact on the business. According to the above, it is understood that the existence of security policies and risk management systems is imperative (Gordon et al., 2003; Kahyaoglu and Caliyurt, 2018). Emphasis on safety should be put in place during the design phase of the systems to prevent subsequent malfunction (Bednar et al., 2013). However, no specific model has been developed for the security management of e-services widely used by businesses (Atoum et al., 2014; Eling and Schnell, 2016).

3 Theoretical foundation and hypotheses

3.1 Advisory role

External or internal auditors carry out IT audits in an enterprise in order to ensure the smooth operation of information systems and to avoid fraud (Merhout and Havelka, 2008). According to Abdolmohammadi and Boss (2010), internal auditors should carry out these audits as they are more closely and directly related to the business. Furthermore, Coram et al. (2008) found that firms with internal audit more easily detect fraud related to misappropriation of business assets than those with external auditors. A few years later, Havelka and Merhout (2013) pointed out that audits are important as they aim at information security and integrity (Herath and Herath, 2018). The same view was

supported by Ransbotham and Mitra (2009), who argued that internal audit can have a positive effect on the firm's security efforts.

According to Van Peursem's (2004) survey of internal auditors' views on their duties in a sample of New Zealand internal auditors, the latter's role is mainly advisory rather than mandatory. Specifying this role, the following year, Van Peursem (2005) conducted interviews that suggest that internal auditors communicate daily with IT staff, thereby reducing the incidence of violations before they have a detrimental impact on the business (Steinbart et al., 2018). Their role is advisory, not interventional, as they do not make their own decisions. As Bou-Raad (2000) pointed out, it is up to management to decide whether to accept the internal auditors' proposals or not. In addition, Stewart and Subramaniam (2010) pointed out that internal audit is largely advisory with the ultimate goal of adding value, which is also confirmed by Dittenhofer (2001) research on behaviour and the role of internal auditors.

Bhattacharyya (2015) claimed that the advisory nature of internal auditors derives from their independence and hence their better understanding of functions in different departments. Similarly, Steinbart et al. (2015) pointed out that the contribution of internal audit to the security of information systems lies in the need for an agent independent of the creation of these systems to audit their proper functioning, a view adopted by Islam et al. (2018). According to The IIA Research Foundation (2015), the contribution of internal audit is critical to the security of electronic processes. Internal audit should annually check for possible vulnerabilities of a company, ensure that it can cope in the event of an accident, and that important information is backed up. The same results were found by Brody and Kearns (2009), since backups and recovery plans are of major importance.

From the above, it can be derived that the advisory role of internal auditors is expected to lead to a reduction in the incidence of violations. Thusly, the first research hypothesis is established:

H_1 The advisory role of internal audit is not inversely related to the number of violations.

3.2 Cooperation

According to Maher and Akers (2003), the expansion of the role of internal auditors also includes acting as consultants in the field of IT. They also stressed the great importance of independence for internal auditors. Finally, the independence of internal auditors lies in performing their work without being influenced by any controlled department (Stoel et al., 2012). Technological innovation in business is a crucial factor for successful implementation of policies and strategies (Santoro et al., 2019; Christofi et al., 2019). Cross-functional innovation demonstrates significant contribution to business due to ongoing diversities based on multi factorial correlations. Furthermore, globalisation of markets makes it imperative for businesses and organisations to work in a broader scale of international proportions (Fjellström et al., 2020). Without carefully implemented technological innovative strategies, businesses are unable to fully exploit the diverse cross-functional innovation perspectives for proactive planning. Fjellström et al. (2020) develop strategic innovation management insights, based on diverse business function-specific cases and proposed an integrated cross-functional model of strategic innovation management. Even earlier than that, Merhout and Havelka (2008) showed that

one of the factors affecting the quality of audits is the simultaneous cooperation between the different departments of the firm, the audited department and top management, as it allows for a better flow of information. Bauer and Estep (2018) emphasised that internal auditors must work with IT experts. The results of their research showed that, when relations between the two parties are good, the audit is effective, as knowledge is shared and debugging is timelier.

From the above, it can be derived that cooperation between internal auditors and IT specialists plays a critical role in security.

Thusly, the second research hypothesis is as follow:

H_2 The cooperation between internal audit and IT professionals is not inversely related to the number of violations.

3.3 Technological knowledge

The role of internal auditors has expanded to include IT knowledge (Stoel et al., 2012). In the research conducted by The IIA Research Foundation (2015) on the ten most important technological risks faced by businesses, internal auditors' technological knowledge came in 8th. Only 10% of respondents had knowledge about technology. The solution to this problem must be found by first assessing the gaps in the internal auditors' level of technological knowledge and then providing them with the appropriate training and the ability to work with IT specialists. For example with the increased utilisation of digitalisation, various markets changed their operations to include technologies and online channels previously considered only as a possible future cost. These digital innovations became dominant disrupting industries and important strategic issues in the wider effort to better perform in global markets by meeting customer needs and reaching out to them 'faster at minimum expense' (Fjellström et al., 2020). Richards et al. (2005) argued that internal auditors should have basic technological knowledge, i.e., software, operating system and networking knowledge, knowledge of safety and risk protection and knowledge of the use of information systems necessary to fulfil their role.

This is an age of globalisation and the continuous incorporation of new technologies into business processes, and Abu-Musa (2008) emphasised that internal auditors need to oversee and fulfil their role with further knowledge of the information systems and technologies they use. Curtis et al. (2009) pointed out the need for internal auditors to have technological know-how in an ever-evolving technological environment in order to more effectively evaluate information systems and identify risks of business fraud. Another conclusion drawn from the research of Wallace et al. (2011) of 636 members of the Institute of Internal Auditors regarding IT audits is that, in addition to IT specialists who often perform such audits, internal auditors will have additional benefits and therefore will need to be knowledgeable about technology. Abdolmohammadi and Boss (2010) argued that internal auditors need to have specialised systems knowledge to assist management in decision-making. It is desirable that they have some formal certification that combines technological and economic knowledge and that their research has a positive impact on IT audits and is statistically significant (Petterson, 2005). There should be more training of internal auditors on technology to reduce the number of violations.

From the above, the following research hypothesis is derived:

H_3 The existence of specialised technological knowledge on the part of internal auditors is not inversely related to the number of violation incidents.

3.4 Policies and standards

Businesses should support their security through information security frameworks. Many of these frameworks can be distinguished as policies, models and practices-procedures-guides (Whitman and Mattord, 2003; Barad and Sharma, 2020). Security policies are a tool of senior management, consistent with the goals and mission of a firm, and include employees' security obligations (Lee and Lee, 2002; Whitman and Mattord, 2003). According to D'Arcy and Hovav (2007) and Whitman et al. (2001), security policies refer to in-depth instructions on maintaining security. The intermediate stage concerns standards which aid policy implementation (D'Arcy and Hovav, 2007). The next step of practice-procedures-guides includes practical guidelines and steps to be followed to implement security policies and standards (Upfold and Sewry, 2005; Whitman and Mattord, 2003).

Various security plans can be used that deal with different security aspects, such as NIST SP 800-30 that deals with security risk management (Fenz et al., 2014) or the *RFC2196 Site Security Handbook*, which provides internet security framework and procedures in SMEs (Upfold and Sewry, 2005). It is better for a company to follow an international standard or framework than to establish safety rules on its own, as these are internationally recognised practices (Upfold and Sewry, 2005). For example, ISO 17799 is an international standard and is the basis for developing security policies (D'Arcy and Hovav, 2007; Tabor, 2009). ISO/IEC 27001 is considered one of the most well-known standards that provide a number of safety-promoting elements to help the business understand what to do. However, the way in which the target should be implemented is not covered, and thus ISO/IEC 27002 was published, which is more targeted at the implementation phase and is auxiliary to official ISO/IEC 27001 (Stewart and Jürjens, 2017). ISO/IEC 27002 adds to ISO 17799, providing general guidelines for implementation and improvement of safety (ISO, 2005). The revised version of ISO/IEC 27001 is ISO/IEC 27005: 2018, which deals with security risk management (ISO, 2018). Generally, ISO standards are the most widely used security standards, as is the COBIT framework, by businesses to maintain the security of their information (Sahibudin et al., 2008). The COBIT framework develops and provides credible guidelines and practices that are used worldwide by auditors, executives and employees to understand the procedures to follow to support security (ITGI, 2007; Sahibudin et al., 2008).

Kayworth and Whitten (2010) conducted interviews with business security executives and argued that internal audit is needed to contribute to security, as it independently evaluates security policies and reports results to senior management. Islam et al. (2018) pointed out that internal audit should consider whether or not security policies are in place. Prior to implementing a strategy aimed at the security of electronic processes, internal audit should independently check that all potential risks have been taken into account and that this strategy is in line with the general business strategy (Kahyaoglu and Caliyurt, 2018).

The above shows that security policies and frameworks are vital in terms of security. Their existence and assurance on the part of internal auditors are crucial, as they will contribute to the development of a security strategy aimed at reducing the incidence of violations. Therefore, the following research hypothesis is derived:

H_4 Internal audit security standards are not inversely related to the number of violations.

3.5 Information and training of personnel

An enterprise may be exposed to external or internal violations in its systems. Internal violations concern its employees, whether intentional or not, and the investigator of these incidents (Abawajy, 2014; Guo et al., 2011; Stanton et al., 2005). Their behaviour may come from being inadequately informed and trained on safety rules (Stewart and Jürjens, 2017). D'Arcy and Hovav (2007) surveyed business employees in the USA and emphasised that the number of violations can be reduced if employees are regularly trained and informed about the safety policies and rules they must adhere to, as the problem cannot be resolved by relying solely on technical issues (e.g., firewalls). Stanton et al. (2005) examined the behaviour of employees in the USA regarding safety and concluded that users do not adhere to the basic safety rules and therefore suggested that further training should be provided.

Abawajy (2014) pointed out the need to brief personnel on safety rules in order to make proper use of the systems and to ensure that violations are reduced. Employees can be informed through leaflets or seminars, or by watching targeted videos or playing educational games. Another way is to simulate an incident, where the IT department collaborating with internal audit sends malicious messages to employees to determine if they will respond to them and then provides information and training. The same view is shared by Thomson and von Solms (1998) and Vrontis et al. (2010) who highlight the need for employee information and training courses that target safety as an imperative factor. According to Ng et al. (2009), employees are critical to the security of online services, as users of information systems need to be careful and adhere to security rules. D'Arcy et al. (2009) emphasised that employee information and training programs can deter violations by informing employees about permissible actions they can take and the consequences of violations. It is understood that these programs help employees better understand security policies (Whitman et al., 2001). Operational monitoring of employees' actions is also thought to contribute positively to the security of online services (D'Arcy et al., 2009).

Werlinger et al. (2009) examined the challenges faced by IT employees in trying to provide as much security as possible in a business. The research took the form of semi-structured interviews with 36 IT security experts in 17 organisations. One of the results of the survey is that there is a lack of security training for employees, so they do not understand much of the dangers that can occur. According to Stafford et al. (2018), internal auditors should check that employees follow safety policies and are trained on safety issues. Their role also lies in identifying employees who are less aware of security policies, and in general, in maintaining business security objectives in accordance with the day-to-day processes that take place. Interviews with professional auditors have found that, by talking to employees, internal auditors can find out if the necessary rules are being followed or can even check their browsing history.

From the above, the following research hypothesis is derived:

H_5 Information and training personnel is not inversely related to the number of violations.

4 Research methodology

4.1 Questionnaire design

Internal audit is an integral and mandatory part of all companies listed on the Athens Stock Exchange. With the aim of examining the variables related to internal audit and affecting security, the sample selected was made exclusively of internal auditors working in entities listed on the Athens Stock Exchange. The questionnaire is the important factor in conducting a survey and it was therefore carefully designed to be clear and understandable. Following a detailed international literature search, an electronic questionnaire was developed on Google Forms, and was then sent by e-mail to entities listed on the Athens Stock Exchange to investigate the relationship between internal auditors and information security experts, the level of technology knowledge of internal auditors, the existence of security policy frameworks and the provision and training of security personnel. The questionnaire had 25 questions that were closed-ended and multiple-choice on a Likert-type scale, where the respondent was asked to state the extent to which the research questions/statements are valid. The aim was to complete it quickly, and for this reason, it was divided into five thematic sections, which are discussed below. The questionnaires were answered by 72 companies.

4.2 Variables

The dependent variable *Y* is considered to be the 'security of electronic services', which is defined as the average score derived from Questions 4 through 6. In particular, Questions 4 and 6 came from the study by Steinbart et al. (2015), and they were aimed at examining security through violations and attacks.

The first independent variable is the 'advisory role of internal auditors', which is defined as the average score of Questions 7 through 9. More specifically, two questions (Questions 7 and 8) came from the Steinbart et al.'s (2015) survey.

The second independent variable is 'cooperation-collaboration' (good relationship) between internal auditors and IT experts, defined as the mean score of Questions 10 through 12, which came from the research of Steinbart et al. (2018).

The third independent variable is 'internal auditors' specialised technological knowledge', defined as the average score of Questions 13 through 16. In particular, these four questions were based on the research of Stoel et al. (2012), and they were aimed at investigating the extent to which internal auditors have specialised technology and security knowledge, as well as the degree to which they are trained if they had lacked technological knowledge. In addition, it was investigated whether or not the internal auditors of the CISA Basic Certification for Security are audited.

The fourth independent variable is 'policies-security standards', defined as the average score of Questions 17 through 21, in Part D. These five questions deal with the policies, standards and security frameworks applicable to each entity. The first four questions (17 to 20) came from the research of Upfold and Sewry (2005), while the last question (Question 21) came from Abu-Musa (2008). These questions explored the extent to which each entity adopts and adheres to specific security standards or frameworks, as well as the existence of a uniform information security policy applicable to the enterprise. They also considered the extent to which internal audit contributes to the implementation of the above.

The fifth independent variable, 'information-education', defined as the average score of Questions 22 to 25, dealt with the training and information programs for staff on electronic security procedures. Initially, Questions 22 and 23, from D'Arcy et al. (2009), examined the extent to which a firm has specific instructions on employees' proper use of information systems, as well as the extent to which the firm provides employees training to keep them informed on the correct issues, use and information security. Next, Question 24, by Upfold and Sewry (2005), examined the extent to which employees are knowledgeable about the business information security policy. Part E concluded with Question 25, by The IIA Research Foundation (2015), on the extent to which internal auditors maintain the mandatory existence of safety briefings.

4.3 Regression model

Since the relationship between the variables X and Y is linear, we will use the following theoretical multiple linear regression model that examines the effect of many independent variables on a dependent variable (Creswell and Poth, 2016):

$$Y = b + b_1 X_1 + + b_2 X_2 + b_3 X_3 + b_4 X_4 + b_5 X_5 + e_i \quad (1)$$

where Y is the dependent variable, X_1, X_2, X_3, X_4, X_5 are the independent variables, while the parameters b_1, b_2, b_3, b_4, b_5 are related to the independent variables and express quantitatively the relationship that exists with the dependent variable, that is, it shows how much the dependent variable is expected to change if the independent variable changes by one unit, since the other parameters remain constant. The b parameter indicates the value of the dependent variable when the prediction variables are equal to zero. Finally, the e_i parameter presents the prediction error (Creswell and Poth, 2016; Katsis et al., 2010). Based on the above, we can define the specific regression model we want to evaluate:

$$\begin{aligned} Security\ of\ online\ services = {} & b + b_1 * Advisory\ role + b_2 * Technological \\ & knowledge + b_3 * Cooperation + b_4 * Policies\ and \\ & standards + b_5 * Information\ and\ training \end{aligned} \quad (2)$$

where b (regression coefficients) informs us of the relationship of electronic security with each forecast variable, as long as the effect of all other forecast variables is constant. If the regression coefficient b has a positive value, then we conclude that, when each one of the independent variables is increased, the mean of the dependent variable is positive. Conversely, when the regression coefficient b has a negative value, we conclude that, when one unit increases each of the independent variables, the mean of the dependent variable is negatively changed.

5 Results

5.1 Demographics

Of the 72 companies surveyed, 17 are in manufacturing (23.6%), 16 in services (22.2%), eight in retail (11.1%), and 8 in consulting and professional services. (11.1%), 6 in manufacturing (8.3%), 6 in technology (8.3%), 5 in food services (6.9%), 3 in health

(4.2%), 2 in banking (2.8%) and 1 in the public sector (1.4%). The majority of businesses have over 250 employees (82.8%) followed by 12 businesses (16.3%) with 50 to 250 employees, while only one company has 10 to 50 employees (1.4%). We also note that 68 of the 72 companies have an annual turnover of more than €50 million (94.4%). We also note that the largest percentage of businesses, 52.8%, have suffered one to five cyber attacks in the last 12 months and 31.9% have suffered six to ten attacks.

The largest percentage (48.6%) answered that none of the incidents measured in Question 4 were detected before the emergence of functional problems, financial or reputation loss, 45.8% answered that one to five of the above cases were detected before they caused functional problems or financial or reputation loss, while 5.6% responded that 6 to 10 incidents were detected before they caused functional problems, financial or reputation loss. Finally, the largest percentage of respondents (33.3%) claimed that violations have increased in the last three years.

5.2 Descriptive statistics

Regarding the advisory role of internal auditors, 39.0% of respondents answered that internal auditors advise 'too much' on the different parts of the business. Also, the largest percentage of businesses, 51.4%, thinks that internal auditors act too much as 'players' of a team and not as law enforcement agencies. Finally, 62.5% of businesses surveyed claimed that internal auditors advise to some extent on the security of information systems and information.

Concerning the cooperation between internal auditors and IT specialists, the overwhelming majority (68.1%) considered that information security experts work with internal auditors to a very small extent to ensure that information systems are secure and reliable. Similarly, 58.3% believed that friction between information security experts and internal auditors is not limited. Finally, 69.4% of respondents considered that the relationship between information security specialists and internal auditors is not very personal and close.

With regard to the level of specialised technological knowledge on the part of internal auditors, 65.3% of the respondents responded that internal auditors' knowledge on the security of information systems is limited to non-existent. Similarly, the overwhelming majority (72.2%) argued that internal auditors have little to no specialised technology knowledge of the systems they use, and 69.4% said that internal auditors' training on information system security is almost absent. Finally, 70.8% of respondents say that CISA certification is held by very few internal auditors.

Regarding the existence of security policies and standards audited by internal auditors, it is revealed that 67.6% of the respondents claimed that there is a large amount of information security policy recorded. In contrast, 55.6% of respondents claimed that they do not satisfactorily use any of the ISO standards (ISO 27001, 27005, etc.). Similarly, 68.1% do not use the COBIT framework to a satisfactory degree and 93.1% do not sufficiently use the NIST SP or *RFC2196: Site Security Handbook* frameworks. Finally, 68.1% of those surveyed claimed that internal auditors give little assessment of compliance with security policies and standards.

Table 1 Descriptive statistics

V1	To what extent do internal auditors advise different departments (such as the IT department) on their profitability?	0 0	7 9.7	15 20.8	28 38.9	22 30.6
	To what extent do internal auditors act as 'players' of a team and not as law enforcement agencies?	0 0	4 5.6	14 19.4	17 23.6	37 51.4
	To what extent are internal auditors involved in the security of information and information systems?	3 4.2	45 62.5	17 23.6	3 4.2	4 5.6
V2	To what extent do information security experts work with internal auditors to ensure the security of information systems?	4 5.6%	45 62.5%	7 9.7%	11 15.3%	5 6.9%
	To what extent is friction between information security experts and internal auditors limited?	1 1.4%	41 56.9%	16 22.2%	9 12.5%	5 6.9%
	To what extent is the relationship between information security specialists and internal auditors characterised as close?	3 4.2%	47 65.3%	12 16.7%	7 9.7%	3 4.2%
V3	To what extent have internal auditors knowledge of the security of information systems?	10 13.9%	37 51.4%	13 18.1%	8 11.1%	4 5.6%
	To what extent have internal auditors specialised technological knowledge of the information systems they use?	21 29.2%	31 43.1%	13 18.1%	4 5.6%	3 4.2%
	To what extent is there training for internal auditors on the security of information systems?	33 45.8%	17 23.6%	18 25.0%	2 2.8%	2 2.8%
	To what extent do internal auditors possess the certification Certified Information Systems Auditor (CISA)?	35 48.6%	16 22.2%	16 22.2%	2 2.8%	3 4.2%
V4	To what extent is there a recorded Information Security Policy?	2 2.8%	10 13.9%	11 15.3%	35 48.6%	13 18.1%
	To what extent does your company use any of the ISO standards (ISO 27001, 27005, etc.)?	24 33.3%	16 22.2%	15 20.8%	14 19.4%	3 4.2%
	To what extent does your company use the COBIT framework?	24 33.3%	25 34.7%	17 23.6%	2 2.8%	4 5.6%
	To what extent does your firm use specific frameworks (such as NIST SP or *RFC2196: Site Security Handbook*)?	41 56.9%	26 36.1%	2 2.8%	1 1.4%	2 2.8%
	To what extent do internal auditors evaluate compliance with security policies-standards?	11 15.3%	38 52.8%	18 25%	1 1.4%	4 5.6%
V5	To what extent does your firm have specific guides that outline what employees are allowed to do with their computers?	1 1.4%	7 9.7%	17 23.6%	28 38.9%	19 26.4%
	To what extent does your firm provide training to help its employees improve their knowledge on information security issues?	13 18.1%	46 63.9%	9 12.5%	1 1.4%	3 4.2%
	To what extent is staff knowledgeable of information security policy?	4 5.6%	26 36.1%	24 33.3%	16 22.2%	2 2.8%
	To what extent do internal auditors ensure staff security briefings are beneficial?	23 31.9%	29 40.3%	9 12.5%	9 12.5%	2 2.8%

In terms of information security training, 65.3% have to a large extent specific guideline that emphasise what employees are allowed to do using their computers. In contrast, 81.9% do not provide a sufficient level of training to help their employees improve their knowledge on computers and information security issues. Similarly, 41.7% of the respondents claimed that the staff is not very familiar with the information security policy. Lastly, 72.2% of those surveyed claimed that internal auditors ensure to a very small extent that staff information programs are mandatory and beneficial.

5.3 Correlations

Correlation testing was performed with the Pearson index. It is found that there is a statistically significant linear correlation between the dependent variable and the 'policy-standards' variable, which is characterised as moderate and positive (r = 0.477, *p*-value < 0.05). In addition, there was a statistically significant linear correlation between the dependent variable and the 'advisory role' variable, which was characterised as strong and positive (r = 0.674, *p*-value < 0.05). Finally, there is no statistically significant correlation of the dependent variable with the other independent variables.

Table 2 Correlations

	Security of online services	*Advisory role*	*Cooperation*	*Technological knowledge*	*Policies and standards*	*Information and training*
Security of online services	1					
Advisory role	0.674	1				
Cooperation	–0.033	–0.329	1			
Technological knowledge	–0.157	–0.478	0.782	1		
Policies and standards	0.477	0.122	0.572	0.584	1	
Information and training	–0.002	–0.266	0.700	0.676	0.572	1

This indicator expresses the correlation as a linear relationship (Creswell and Poth, 2016). It is found that there is a statistically significant linear correlation between the dependent variable and the 'policies-standards' variable, which is characterised as moderate and positive (r = 0.477, *p*-value < 0.05). In addition, there was a statistically significant linear correlation between the dependent variable and the 'advisory role' variable, which was characterised as strong and positive (r = 0.674, *p*-value < 0.05). Finally, there is no statistically significant correlation of the dependent variable with the other independent variables. The results also depicts that the variables associated with the dependent variable, namely the 'policy-standards' variable and the 'advisory role' variable, have no relation to each other. Moreover, the 'information-education' variable is not associated with any variable, while the 'technological knowledge' variable is moderately correlated with two other variables. Finally, the variable 'cooperation' is significantly correlated with the other three variables.

5.4 Regression analysis

5.4.1 Reliability analysis

The questionnaire questions were grouped into factors conceptually and the reliability of each scale was tested using the Cronbach's alpha. Table 3 presents the variables as well as their reliability index.

Table 3 Cronbach's alpha

	Average	*Cronbach's alpha*
Advisory role	4.0556	0.861
Cooperation	2.5556	0.922
Technological knowledge	2.1007	0.945
Policies and standards	2.0938	0.736
Information and training	2.7083	0.743

According to Kline (1999), good reliability is indicated when the value of the alpha coefficient is above 0.7. As Table 3 shows, all Cronbach's alpha values are above 0.7, so all question scales are reliable.

5.4.2 Multiple linear regression analysis

In the model, it is found that 65% of variance of e-services security is interpreted by the independent variables, while the remaining 35% is interpreted by other factors (Creswell and Poth, 2016; Katsis et al., 2010).

Based on the *B* values, the regression equation is modelled as follows:

$$\begin{aligned} \textit{Security of online services} = {} & 1.438 + 0.416 * \textit{Advisory role} + 0.044 * \textit{Cooperation} \\ & -0.175 * \textit{Technological knowledge} + 0.605 * \textit{Policies} \\ & \textit{and standards} + 0.170 * \textit{Information and training} \end{aligned} \quad (3)$$

Table 4 Coefficients

Model		*Unstandardised coefficients*		*Standardised coefficients*	*t*	*Sig.*
		B	*Std. error*	*Beta*		
1	(Constant)	1.438	.433		3.324	.001
	Advisory role	.416	.087	.481	4.787	.000
	Cooperation	.044	.105	.051	.413	.681
	Technological knowledge	–.175	.116	–.222	–1.508	.136
	Policies and standards	.605	.113	.613	5.348	.000
	Information and training	–.170	.107	–.162	–1.584	.118

Based on the *t* and sig. values, our research hypotheses will be accepted or rejected. Table 4 shows that for the first independent variable 'advisory role' (t_1 = 4.787 and sig. = *p*-value = 0.000 < 0.05) and the fourth independent variable 'policies and standards' (t_4 = 5.348 and sig. = *p*-value = 0.000 < 0.05), the null hypothesis is rejected and therefore the variables 'advisory role' and 'policies-standards' affects the security of

online services. On the contrary, for the independent variables 'cooperation' (t_2 = 0.413 and sig. = p-value = 0.681 > 0.05), 'technological knowledge' (t_3 = –1.508 and sig. = p-value = 0.136 > 0.05) and 'information-training' (t_5 = –1.584 and sig. = p-value = 0.118 > 0.05), we accept the null hypothesis and therefore these variables do not affect the security of online services. The results for the research hypotheses are presented in Table 5.

Table 5 Research hypotheses

Zero hypothesis H_0	*Conclusion*
The advisory role of internal audit is not inversely related to the number of violations.	Rejected
The good relationship between internal audit and IT experts is not inversely related to the number of violations.	Confirmed
The existence of specialised technological knowledge on the part of internal auditors is not inversely related to the number of violations.	Confirmed
Internal audit security standards are not inversely related to the number of violations.	Rejected
Information and training of security personnel is not inversely related to the number of violations.	Confirmed

It also turns out that there is no multigrid issue, since VIF < 10 for all independent variables. In addition, it confirms the absence of polylinearity, since the values of the eigenvalue are less than 10 and the condition index is less than 30 for all independent variables (Katsis et al., 2010). Therefore, our model does not suffer from the problem of polygraph.

6 Discussion

Concerning the advisory role of internal auditors, the majority of respondents argued that internal auditors operate to a large extent in other departments, such as IT. However, the good relationship between IT specialists and internal auditors is argued to be quite limited, resulting in friction between the two parts. In addition, the majority of respondents responded that the level of specialised technological knowledge on the part of internal auditors is very low. Regarding the security policies-standards audited by internal audit, it appears that the majority of companies has some recorded information security policy, but do not satisfactorily implement some of the key security standards and frameworks (ISO, COBIT, etc.). Finally, with regard to information and training of personnel on security issues, the majority of respondents stated that, although businesses have sufficiently specific guidelines on how to make good use of online services, no training is provided to staff, and internal auditors do not ensure that information and training programs are mandatory.

In order to extract more specialised results, the correlations between variables and regression analysis were performed. The results showed that only 2 of the 5 independent variables in the model were statistically significant. In particular, it was found that there was a statistically significant linear positive correlation between the dependent variable (security of electronic services) and the independent variables 'advisory role' and 'policies-standards'. The above findings are consistent with Bhattacharyya (2015) and

Van Peursem (2004), who pointed out the benefits of the guidance-counselling role of internal audit, but also with Islam et al. (2018), who emphasised that internal audit needs to consider security policies to achieve maximum security.

Concerning the variable 'technological knowledge', the regression also showed that this variable is not statistically significant and therefore does not affect the security of electronic services. These findings contradict the pre-existing literature, as Abu-Musa (2008) and Curtis et al. (2009) argued that the existence of specialised technological knowledge on the part of internal auditors will enhance their role in detecting possible infringements in information systems. This finding could imply a separation of auditing and technical knowledge in the respondent's opinion, thusly indicating a limitation of internal audit perspective of its fundamental role as a tool for control over the activities of an organisation. An audit is divided in types as it is for example a financial or a technical audit. Auditors are required to cover a wide range of expertise beyond strictly accounting or financial knowledge (Papastathis, 2014). It is understandable that in specific cases experts should be used to back the auditor's report. However, a certain degree of different areas of expertise knowledge is required from the auditor.

The independent variable 'cooperation' has to do with the good relationship between cyber security experts and internal auditors. The regression also showed that the variable 'collaboration' is not statistically significant and therefore does not affect the security of online services. This result is inconsistent with the studies by Bauer and Estep (2018), Steinbart et al. (2018), Caputo et al. (2018) and Fjellström et al. (2020), who argued that collaboration leads to knowledge sharing and that more violations are detected before they cause financial or other loss to the business. It is evident that similarly to findings regarding 'technical knowledge', auditors perceive cyber auditing as a separate field from their line of work. Such a finding would have be understandable, but not to the degree that technical and cyber audits are performed without the auditor's supervision.

The fifth independent variable in the model concerns information training of security personnel, and according to the regression, the variable is not statistically significant and therefore does not affect the security of online services. This result is inconsistent with similar findings arguing that training (Caputo et al., 2018) and information security workers (Abawajy, 2014; D'Arcy and Hovav, 2007) are catalytic, as they lead to a reduction in incidents of abuse. It is possible that the significance of cyber security is validated in the responses received from the questionnaire. However, the intriguing part of this research is the inability of correlating cyber security with technical knowledge, cooperation with security experts and training.

Summarising all of the above findings, the two variables found significant to the security of electronic services, were company policies and the auditor's advisory role. Regarding policies, the literature confirms that an internal auditor is valuable for the formation of regulations and safety of procedures. The close cooperation between top management and audit is vital to formulate policies containing safety measures as well as serving organisational goals of efficiency and profitability. The same can be understood for the auditors' advisory role from the organisational chart of the company, and the auditors placement in it.

The other three factors do not appear to be linearly related to the security of online services, but may have some other form of relationship. Considering the variables whose correlations were not significant, an interesting subject is highlighted. In today's economy and globalised market, the swiftness of innovation in matters of technology, communication and facilitation of activities is evident. This expansion of information

requires from auditors to grasp a better understanding of technology and its procedures. In order to perform thorough audits, internal auditors must consider the modern sources of deceit. To an extent, the facilitation offered by technology also creates new threats, as data are no longer secured inside a physical space. As auditors are in charge of evaluating procedures and their safety, it is their task to strive to include and cover cyber security safety measures in an audits list of activities (Sabillon, 2018). On the other hand, the complexity of cyber audit may impose different tactics in dealing with modern technological risks. It is possible that audit with its traditional philosophy and form is insufficient. However, audit redesigns or its necessary new forms require time and research to be verified and consolidated.

7 Conclusions, implications and future research

The security of online services and information systems is imperative for all businesses in a time when everything is digitalised. Internal audit has changed and enriched its responsibilities and it should also contribute to the security of online services in a variety of ways. The results of the extensive research overview outline the crucial role of internal audit in the security of information systems. The conclusions drawn from empirical research are quite significant. Initially, the majority of businesses are classified as large companies and the incidents of infringement in these businesses are real and tend to increase over time. Training of auditors is imperative, in light of the close relation between security and guidelines provided by each company. Furthermore, auditors need to deepen their knowledge on issues of cyber security in order to improve their collaboration with field experts. Auditors' consulting role and their collaboration with management in forming policies remains vital for cyber security measures. On the other hand, it is evident that today, auditors training in cyber security risk avoidance may prove less that efficient in real cybernetic attack scenarios. Audit remains a strong tool for efficiency and reliability in a company. However, which role audit is going to take regarding the digitisation's era is to be decided by the capability of auditors to include cyber safety into their portfolio of activities.

This research highlights the necessity for audit and auditors to broaden their knowledge on cyber safety in order to succeed in digitised audit efficiency. Both the needs for closer cooperation with the technical staff, and to safeguard companies from cyber attacks, highlight the significance of this issue. Some factors differ from the existing literature. This can be translated by the swiftness with which technology is evolving as well as the range of different knowledge auditors are required to acquire regarding cyber audits.

In terms of future research avenues, it would be prudent to carry out a future survey with an even bigger sample, possibly a multinational one to allow for greater accuracy, comparative conclusions and a greater degree of generalisation. Furthermore, the reasons why technological training, knowledge and cross-department cooperation were not found important in terms of service security, need to be further studied. More specifically, it should be investigated whether this is consequent to low levels of collaboration between the audit and IT department. Or, alternatively, whether the phenomenon is influenced by factors resulting from outsourcing, or the shift of responsibilities to other departments due to the nature of the audit.

References

Abawajy, J. (2014) 'User preference of cyber security awareness delivery methods', *Behaviour & Information Technology*, Vol. 33, No. 3, pp.237–248.

Abdolmohammadi, M.J. and Boss, S.R. (2010) 'Factors associated with IT audits by the internal audit function', *International Journal of Accounting Information Systems*, Vol. 11, No. 3, pp.140–151.

Abu-Musa, A.A. (2008) 'Information technology and its implications for internal auditing', *Managerial Auditing Journal*, Vol. 23, No. 5, pp.436–466.

Alali, M., Almogren, A., Hassan, M.M., Rassan, I.A. and Bhuiyan, M.Z.A. (2018) 'Improving risk assessment model of cyber security using fuzzy logic inference system', *Computers & Security*, Vol. 74, No. 2018, pp.323–339.

Atoum, I., Otoom, A. and Ali, A.A. (2014) 'A holistic cyber security implementation framework', *Information Management & Computer Security*, Vol. 22, No. 3, pp.251–264.

Barad, S. and Sharma, P. (2020) 'A study of security audit and VAPT audit and implementation of cyber security controls like WSUS against cyber threats', *Journal of Engineering Sciences*, Vol. 11, No. 4, pp.1047–1054.

Bauer, T. and Estep, C. (2018) *One Team or Two? Investigating Relationship Quality Between Auditors and IT Specialists: Implications for Audit Team Identity and the Audit Process* [online] https://ssrn.com/abstract=2579198 (accessed 5 February 2019).

Bednar, P., Sadok, M. and Katos, V. (2013) 'Contextual dependencies in information systems security. AIS SIGSEC and IFIP TC 11.1', *Workshop on Information Security & Privacy, WISP 2013*, Milan, Italy.

Bhattacharyya, A.K. (2015) *Internal Audit – Its Role in Corporate Governance* [online] https://ssrn.com/abstract=2621149 (accessed 5 February 2019).

Bou-Raad, G. (2000) 'Internal auditors and a value-added approach: the new business regime', *Managerial Auditing Journal*, Vol. 15, No. 4, pp.182–187.

Brody, R.G. and Kearns, G. (2009) 'IT audit approaches for enterprise resource planning systems', *ICFAI Journal of Audit Practice*, Vol. 6, No. 2, pp.7–26.

Broom, A. (2009) 'Security consolidation and optimisation: gaining the most from your IT assets', *Computer Fraud & Security*, Vol. 2009, No. 5, pp.15–17.

Caputo, F., Evangelista, F. and Russo, G. (2018) 'The role of information sharing and communication strategies for improving stakeholder engagement', in Shams, S., Vrontis, D., Weber, Y. and Tsoukatos, E. (Eds.): *Business Models for Strategic Innovation*, pp.25–43, Routledge, London [online] https://doi.org/10.4324/9781351257923.

Cebula, J.J. and Young, L.R. (2010) *A Taxonomy of Operational Cyber Security Risks*, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA.

Chebbi, H., Yahiaoui, D., Thrassou, A. and Vrontis, D. (2013) 'The exploration activity's added value into the innovation process', *Global Business and Economics Review*, Vol. 15, Nos. 2–3, pp.265–278.

Christofi, M., Vrontis, D., Thrassou, A. and Shams, S.R. (2019) 'Triggering technological innovation through cross-border mergers and acquisitions: a micro-foundational perspective', *Technological Forecasting and Social Change*, Vol. 146, No. 2019, pp.148–166.

Clark, M. and Harrell, C.E. (2013) 'Unlike chess, everyone must continue playing after a cyber-attack', *Journal of Investment Compliance*, Vol. 14, No. 4, pp.5–12.

Cohen, A. and Sayag, G. (2010) 'The effectiveness of internal auditing: an empirical examination of its determinants in Israeli organisations', *Australian Accounting Review*, Vol. 20, No. 3, pp.296–307.

Coram, P., Ferguson, C. and Moroney, R. (2008) 'Internal audit, alternative internal audit structures and the level of misappropriation of assets fraud', *Accounting and Finance*, Vol. 48, No. 4, pp.543–559.

Creswell, J.W. and Poth, C.N. (2016) *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*, Sage Publications, USA.

Curtis, M.B., Jenkins, J.G., Bedard, J.C. and Deis, D.R. (2009) 'Auditors' training and proficiency in information systems: a research synthesis', *Journal of Information Systems*, Vol. 23, No. 1, pp.79–96.

D'Arcy, J. and Hovav, A. (2007) 'Deterring internal information systems misuse', *Communications of the ACM*, Vol. 50, No. 10, pp.113–117.

D'Arcy, J., Hovav, A. and Galletta, D. (2009) 'User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach', *Information Systems Research*, Vol. 20, No. 1, pp.79–98.

Da Veiga, A. and Eloff, J.H.P. (2007) 'An information security governance framework', *Information Systems Management*, Vol. 24, No. 4, pp.361–372.

Dittenhofer, M. (2001) 'Internal auditing effectiveness: an expansion of present methods', *Managerial Auditing Journal*, Vol. 16, No. 8, pp.443–450.

Drogalas, G., Arampatzis, K. and Anagnostopoulou, E. (2016) 'The relationship between corporate governance, internal audit and audit committee: empirical evidence from Greece', *Corporate Ownership & Control*, Vol. 14, Nos. 1–4, pp.569–577.

Drogalas, G., Karagiorgos, T. and Arampatzis, K. (2015) 'Factors associated with internal audit effectiveness: evidence from Greece', *Journal of Accounting and Taxation*, Vol. 7, No. 7, pp.113–122.

Eling, M. and Schnell, W. (2016) 'What do we know about cyber risk and cyber risk insurance?', *The Journal of Risk Finance*, Vol. 17, No. 5, pp.474–491.

Fenz, S., Heurix, J., Neubauer, T. and Pechstein, F. (2014) 'Current challenges in information security risk management', *Information Management & Computer Security*, Vol. 22, No. 5, pp.410–430.

Fielden, K. (2011) 'An holistic view of information security: a proposed framework', *International Journal of Infonomics*, Vol. 4, Nos. 1/2, pp.427–434.

Fjellström, D., Osarenkhoe, A., Pettersson, T. and Tadesse, D. (2020) 'The role of digitalization in smes' strategy development: the case of Sweden', in Thrassou, A., Vrontis, D., Weber, Y., Shams, S.R. and Tsoukatos, E. (Eds.): *The Changing Role of SMEs in Global Business: Volume I: Paradigms of Opportunities and Challenges*, *Palgrave Studies in Cross-disciplinary Business Research, in Association with EuroMed Academy of Business*, pp.65–88, Palgrave Macmillan, Cham, DOI: 10.1007/978-3-030-45831-7.

Giacomarra, M., Crescimanno, M., Sakka, G. and Galati, A. (2019) 'Stakeholder engagement toward value co-creation in the F&B packaging industry', *EuroMed Journal of Business*, Vol. 15, No. 3, pp.315–331 [online] https://doi.org/10.1108/EMJB-06-2019-0077.

Gordon, L.A., Loeb, M.P. and Sohail, T. (2003) 'A framework for using insurance for cyber-risk management', *Communications of ACM*, Vol. 46, No. 3, pp.81–85.

Guo, K.H., Yuan, Y., Archer, N.P. and Connelly, C.E. (2011) 'Understanding nonmalicious security violations in the workplace: a composite behavior model', *Journal of Management Information Systems*, Vol. 28, No. 2, pp.203–236.

Hannaford, C.S. (1995) 'Can computer security really make a difference?', *Managerial Auditing Journal*, Vol. 10, No. 5, pp.10–15.

Havelka, D. and Merhout, J.W. (2013) 'Internal information technology audit process quality: theory development using structured group processes', *International Journal of Accounting Information Systems*, Vol. 14, No. 3, pp.165–192.

Herath, H.S. and Herath, T.C. (2018) 'Post-audits for managing cyber security investments: Bayesian post-audit using Markov chain Monte Carlo (MCMC) simulation', *Journal of Accounting and Public Policy*, Vol. 37, No. 6, pp.545–563.

Islam, M.S., Farah, N. and Stafford, T.F. (2018) 'Factors associated with security/cybersecurity audit by internal audit function: an international study', *Managerial Auditing Journal*, Vol. 33, No. 4, pp.377–409.

ISO (2005) *ISO/IEC 27002:2005, Information Technology – Security Techniques – Code of Practice for Information Security Controls* [online] https://www.iso.org/standard/50297.html (accessed 5 February 2019).

ISO (2018) *ISO/IEC 27005:2018, Information Technology – Security Techniques – Information Security Risk Management* [online] https://www.iso.org/standard/75281.html (accessed 5 February 2019).

ITGI (2007) *COBIT 4.1: Control Objectives for Information and Related Technology*, IT Governance Institute, Rolling Meadows, IL.

Kahyaoglu, S.B. and Caliyurt, K. (2018) 'Cyber security assurance process from the internal audit perspective', *Managerial Auditing Journal*, Vol. 33, No. 4, pp.360–376.

Katsis, Y., Deutsch, A., Papakonstantinou, Y. and Vassalos, V. (2010) 'Inconsistency resolution in online databases', in *2010 IEEE 26th International Conference on Data Engineering (ICDE 2010)*, IEEE, March, pp.1205–1208.

Kayworth, T. and Whitten, D. (2010) 'Effective information security requires a balance of social and technology factors', *MIS Quarterly Executive*, Vol. 9, No. 3, pp.163–175.

Khlif, H. and Guidara, A. (2018) 'Quality of management schools, strength of auditing and reporting standards and tax evasion', *EuroMed Journal of Business*, Vol. 13, No. 2, pp.149–162.

Kline, P. (1999) *The Handbook of Psychological Testing*, 2nd ed., Routledge, London.

Lee, J. and Lee, Y. (2002) 'A holistic model of computer abuse within organizations', *Information Management & Computer Security*, Vol. 10, No. 2, pp.57–63.

Lois, P., Drogalas, G., Karagiorgos, A. and Chlorou, A. (2019a) 'Tax compliance during fiscal depression periods: the case of Greece', *EuroMed Journal of Business*, Vol. 14, No. 3, pp.274–291.

Lois, P., Drogalas, G., Karagiorgos, A. and Tsikalakis, K. (2019b) 'Internal audits in the digital era: opportunities, risks and challenges', *EuroMed Journal of Business*, Vol. 15, No. 2, pp.205–217, Emerald Publishing Limited, ISSN: 1450-2194.

Maher, M. and Akers, M.D. (2003) 'Internal audit's role in systems development: the CEO's perspective', *Internal Auditing*, Vol. 18, No. 1, pp.35–39.

Merhout, J.W. and Havelka, D. (2008) 'Information technology auditing: a value-added IT governance partnership between IT management and audit', *Communications of the Association for Information Systems*, Vol. 23, No. 26, pp.463–482.

Ng, B., Kankanhalli, A. and Xu, Y. (2009) 'Studying users' computer security behavior: a health belief perspective', *Decision Support Systems*, Vol. 46, No. 4, pp.815–825.

Papastathis, P. (2014) *Modern Internal Audit and its Practical Implementation*, Printfair Publications, Athens.

Petterson, M. (2005) 'The keys to effective IT auditing', *The Journal of Corporate Accounting & Finance*, Vol. 16, No. 5, pp.41–46.

Ransbotham, S. and Mitra, S. (2009) 'Choice and chance: a conceptual model of paths to information security compromise', *Information Systems Research*, Vol. 20, No. 1, pp.121–139.

Richards, D.A., Oliphant, A.S. and Le Grand, C.H. (2005) *Global Technology Audit Guide: Information Technology Controls*, Institute of Internal Auditors, Altamonte Springs, FL.

Sabillon, R. (2018) 'A practical model to perform comprehensive cybersecurity audits', *Enfoque UTE*, Vol. 9, No. 1, pp.127–137.

Sahibudin, S., Sharifi, M. and Ayat, M. (2008) 'Combining ITIL, COBIT and ISO/IEC 27002 in order to design a comprehensive IT framework in organizations', Paper presented at the *Second Asia International Conference on Modelling & Simulation*, Malaysia, May [online] https://ieeexplore.ieee.org/document/4530569 (accessed 5 February 2019).

Santoro, G., Ferraris, A. and Winteler, D.J. (2019) 'Open innovation practices and related internal dynamics: case studies of Italian ICT SMEs', *EuroMed Journal of Business*, Vol. 14, No. 1, pp.47–61 [online] https://doi.org/10.1108/EMJB-05-2018-0031.

Sarens, G. and De Beelde, I. (2006) 'Internal auditors' perception about their role in risk management: a comparison between US and Belgian companies', *Managerial Auditing Journal*, Vol. 21, No. 1, pp.63–80.

Shams, S.M.R., Vrontis, D., Weber, Y. and Tsoukatos, E. (2018) 'Strategic innovation management', in Shams, S., Vrontis, D., Weber, Y. and Tsoukatos, E. (Eds.): *Business Models for Strategic Innovation*, pp.1–10, Routledge, London [online] https://doi.org/10.4324/9781351257923.

Siouziou, I., Toudas, K. and Menexiadis, M. (2017) 'Internal audit and systems of internal audit in Greek banks', *China-USA Business Review*, Vol. 16, No. 12, pp.576–587.

Souppaya, M. and Scarfone, K. (2013) *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*, NIST Special Publication 800-83 [online] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf (accessed 5 February 2019).

Stafford, T., Deitz, G. and Li, Y. (2018) 'The role of internal audit and user training in information security policy compliance', *Managerial Auditing Journal*, Vol. 33, No. 4, pp.410–424.

Stanton, J.M., Stam, K.R., Mastrangelo, P. and Jolton, J. (2005) 'An analysis of end-user security behaviors', *Computers & Security*, Vol. 24, No. 2, pp.124–133.

Steinbart, P.J., Raschke, R.L., Gal, G. and Dilla, W.N. (2015) *The Influence of Internal Audit on Information Security Effectiveness: Perceptions of Internal Auditors* [online] https://dx.doi.org/10.2139/ssrn.2685943 (accessed 5 February 2019).

Steinbart, P.J., Raschke, R.L., Gal, G. and Dilla, W.N. (2018) 'The influence of a good relationship between the internal audit and information security functions on information security outcomes', *Accounting, Organizations and Society*, in press.

Stewart, H. and Jürjens, J. (2017) 'Information security management and the human aspect in organizations', *Information & Computer Security*, Vol. 25, No. 5, pp.494–534.

Stewart, J. and Subramaniam, N. (2010) 'Internal audit independence and objectivity: emerging research opportunities', *Managerial Auditing Journal*, Vol. 25, No. 4, pp.328–360.

Stoel, D., Havelka, D. and Merhout, J.W. (2012) 'An analysis of attributes that impact information technology audit quality: a study of IT and financial audit practitioners', *International Journal of Accounting Information Systems*, Vol. 13, No. 1, pp.60–79.

Tabor, S.W. (2009) 'Exploring the role of frameworks & methodologies in information security management & governance – research in progress', *Proceedings of the 15th Americas Conference on Information Systems*, San Francisco, CA, August [online] https://www.researchgate.net/publication/220894066_Exploring_the_Role_of_Frameworks_Methodologies_in_Information_Security_Management_Governance_-_Research_in_Progress (accessed 5 February 2019).

The IIA Research Foundation (2015) *Navigating Technology's Top 10 Risks – Internal Audit's Role* [online] https://www.iia.nl/SiteFiles/Publicaties/Navigating%20Technology's%20Top%2010%20Risks%20_Small.pdf (accessed 5 February 2019).

Thompson, D. (1998) '1997 computer crime and security survey', *Information Management & Computer Security*, Vol. 6, No. 2, pp.78–101.

Thomson, M.E. and Von Solms, R. (1998) 'Information security awareness: educating your users effectively', *Information Management & Computer Security*, Vol. 6, No. 4, pp.167–173.

Trim, P.R.J. and Lee, Y.I. (2010) 'A security framework for protecting business, government and society from cyber attacks', in *IEEE 5th International Conference on System of Systems Engineering (SoSE)*, UK, June [online] https://ieeexplore.ieee.org/document/5544085 (accessed 5 February 2019).

Upfold, C.T. and Sewry, D.A. (2005) 'An investigation of information security in small and medium enterprises (SMEs) in the Eastern Cape', in Venter, H.S. et al. (Eds.): *Proceedings of the ISSA 2005 New Knowledge Today Conference*, South Africa, 29 June–1 July, Article 082, pp.1–17 [online] https://www.researchgate.net/publication/33996619_An_investigation_of_information_security_in_small_and_medium_enterprises_SME's_in_the_Eastern_Cape (accessed 5 February 2019).

Van Peursem, K. (2004) 'Internal auditors' role and authority: New Zealand evidence', *Managerial Auditing Journal*, Vol. 19, No. 3, pp.378–393.

Van Peursem, K. (2005) 'Conversations with internal auditors: the power of ambiguity', *Managerial Auditing Journal*, Vol. 20, No. 5, pp.489–512.

Vrontis, D., Thrassou, A. and Zin, R.M. (2010) 'Internal marketing as an agent of change – implementing a new human resource information system for Malaysian Airlines', *Journal of General Management*, Vol. 36, No. 1, pp.21–41.

Wallace, L., Lin, H. and Cefaratti, M.A. (2011) 'Information security and Sarbanes-Oxley compliance: an exploratory study', *Journal of Information Systems*, Vol. 25, No. 1, pp.185–211.

Werlinger, R., Hawkey, K. and Beznosov, K. (2009) 'An integrated view of human, organizational, and technological challenges of IT security management', *Information Management & Computer Security*, Vol. 17, No. 1, pp.4–19.

Whitman, M. and Mattord, H. (2003) *Principles of Information Security*, 1st ed., Thomson Course Technology, Boston.

Whitman, M.E., Townsend, A.M. and Alberts, R.J. (2001) 'Information systems security and the need for policy', in Khosrowpour, M. (Ed.): *Information Security Management: Global Challenges in the New Millennium*, pp.9–18, Idea Group Publishing, Hershey, PA.

Yeboah-Ofori, A. and Islam, S. (2019) 'Cyber security threat modeling for supply chain organizational environments', *Future Internet*, Vol. 11, No. 3, p.63.

Zakaria, K.N., Othman, S.H. and Zainal, A. (2019) 'Review of cybersecurity audit management and execution approaches', in *2019 6th International Conference on Research and Innovation in Information Systems (ICRIIS)*, IEEE, pp.1–6.