Audit financiar, XIV, Nr. 6(138)/**2016**, *670-679*
ISSN: 1583-5812; ISSN on-line: 1844-8801

Information security – a new challenge for the young and future financial auditors

Sînziana-Maria RÎNDAŞU,
Bucharest University of Economic Studies,
E-mail: sinziana_rindasu@yahoo.com

Abstract

The purpose of this paper is to inquire if the young and future financial auditors are fully aware of the impact that information security has on audit missions, focusing also on the responsibilities of the participants in financial audit missions, regarding the assessment of the risks derived from information security. To determine the extent to which audit risk might be influenced by information security, a literature review was conducted, that has focused on this current concern, as expressed by different researchers, professional bodies, Big Four companies and the regulators. In order to assess the current level of awareness regarding the impact of information security on the audit risk, 25 young professionals have participated to a survey and with their answers have proven that they realize the impact of information securing on audit missions and the necessity of having sufficient knowledge regarding information technology in order to identify the risk from the information security area which might affect the financial statements and the activity of the organization. Moreover, young and future financial auditors are aware of the fact that the audit profession will suffer modifications due to the changes in the information technology field, which will affect the approaches in audit missions and in this regards the financial auditors must develop new working skills such as understanding information systems and information security and possessing skills in analysis and data modelling. Besides the survey used, five auditors who work in Big Four companies were interviewed, in order to highlight the way in which the profession is adapting to technological changes, especially in the case of assessing controls of information technology systems and information security. From the results of the interview it can be concluded that within the Big Four companies, there is a high level of awareness regarding the necessity of solid knowledge in the information technology field. The paper is the first to examine the perception of young and future financial auditors from Romania, regarding the impact that the information security has on audit missions.

Keywords: *Financial audit, information security, information technology, lifelong learning.*

JEL Classification: *M41, M42, M15.*

To cite this article:
Rîndaşu, S.M. (2016), Information security – a new challenge for the young and future financial auditors, Audit Financiar, vol. XIV, no. 6(138)/2016, pp. 670-679, DOI: 10.20869/AUDITF/2016/138/670

To link to this article:
http://dx.doi.org/10.20869/AUDITF/2016/138/670

Introduction

We live and operate in an era which is continuously improving and the change is present in any activity field, especially in the financial and accounting field. Lately, more and more professional bodies such as the Association of Chartered Certified Accountants (ACCA), Institute of Management Accountants (IMA), Institute of Chartered Accountants in England and Wales (ICAEW) and Centre for Audit Quality (CAQ), and also regulatory bodies such as the Securities and Exchange Commission (SEC) have raised the issue of the knowledge that a financial auditor must possess in certain areas of the information technology (IT) field, such as: *big data* concepts, *data mining* analysis (ACCA, 2013), knowledge necessary to analyse and understand information security and the way in which it might affect the activity of a company (ACCA, 2015; ICAEW, 2015).

The impact that the information security has on the objectives and activities of the companies, such as losing confidential data, which might affect the reputation of a company and decrease the level of the investors' trust frequently determines the need for financial auditors to possess solid knowledge in order to understand how the information systems within the organization are working and also how information security in maintained.

Because of the expansion in information technology area, which involves the use of information systems in almost any activity of the companies, it is no longer sufficient for the financial auditors to focus on the financial statements; they must also consider the internal controls of the information systems which might affect the financial information and the activity of the company. It is not enough for the auditors to understand the flows of the information systems, they also have to make sure about the existence of efficient controls which verify the information security (Chorafas, 2008; CAQ, 2014a, b).

According to the Public Company Accounting Oversight Board (PCAOB) Auditing Standard No. 12 (PCAOB, 2010), the external auditor needs to understand both the company's activity and the information systems of the organization, which might be able to affect the accuracy of the financial data or are likely to have a significant impact on the operational activities.

The risk assigned to information systems is a key component, which must be taken into consideration when the audit risk is established. Another important issue is the fact that financial auditors do not have to understand all the information processes within a company, but only those information processes that might affect the financial data or the activity of the company.

Currently there are no clear regulations at national or international level regarding the extent to which financial auditors need to understand the information systems and security. More and more professional bodies and Big Four companies have conducted a series of studies from which it has been proven the necessity for financial auditors to understand information security.

The purpose of this paper is to highlight how this new challenge – the knowledge on information security – is understood by the young and future financial auditors and what is the possible impact on the profession over the next years.

1. Literature review

Recently, the issue of the information security impact on the companies and its importance for financial auditors has been addressed by professional bodies (ACCA, CIMA, ICAEW and CAQ) and regulatory bodies (SEC). The financial accounting field is changing rapidly (Stanciu, 2015) and auditors need to adapt to these changes in the information technology field which might alter the profession, through a continuous improvement of their skills and knowledge.

The continuous improvement of the skills and knowledge of financial auditors is a continuous process in the actual economic context. The process starts from the academic environment that should offer a proper education regarding current practices and must adapt to the current necessities of the business environment (Albu and Toader, 2012).

The changes in the financial audit field were felt more acutely after 2002 when the Sarbanes-Oxley Act introduced new regulations for the profession, claiming that auditors need to possess sufficient knowledge in order to assess correctly the controls of the information systems that might influence the accuracy of financial statements. Moreover, in this current economic environment, it is not enough for auditors to base their training only on the financial accounting field. Both external and internal auditors must have solid knowledge in the information technology field (Chorafas, 2008).

In Romania, the financial and accounting practitioners use information systems in almost any part of their activity and are aware of the necessity to possess sufficient knowledge regarding the IT and communication field, but the current regulations and curricula of the national professional bodies are not yet aligned with the international professional bodies' standards and best practices (Tudor et al., 2013). In this regard, it is expected that in the next years, the Romanian professional bodies from the financial and accounting field will modify the existing *curricula*, by introducing new study programs in the information technology field.

Information security is considered to be a new element with a significant impact on the profession, due to the fact that it highlights new risk areas and, in this regard, the financial auditors must assess both the risks of the information systems and the issues of information security. The 2013 ACCA report, "Digital Darwinism: thriving in the face of technology change", focuses on the need to be aware of the changes that might affect the profession. In 2015, another study from the same professional body emphasises the fact that financial professionals are more aware of the impact that information security has over the companies (ACCA, 2015). By comparing the results of this study with the previous studies between 2012 and 2014, it can be noticed the fact that, globally, financial and accounting professionals are becoming more responsible regarding the changes which might affect their activity.

In 2016, ACCA in collaboration with IMA focused on the impact of cybercrime and the way in which practitioners from the financial accounting field must act, by: making reasonable assessments on the financial impact that security breaches might have over the company, defining a strategy regarding risk, and helping the company to prioritize the security of the most important digital assets against specific attacks. Furthermore, the study presents the specific risks that might occur in the case of a threat that targets the company or the clients' data, having in this instance an increase of the operational and financial risks.

From the research conducted by ACCA and IMA in 2016 it has been concluded that both the auditors and the other practitioners from the financial field understand the need to develop their knowledge in the IT field, considering the possibility that in the future there will be more hybrid jobs within the companies, in which the financial accounting professionals will be able to understand and work efficiently with information systems, being capable of maintaining and verifying the information security. The future of the audit profession is somehow questionable, audit being one of the fields that might disappear because of computerization, while hybrid fields between audit and information technology have a much lower probability to be replaced by the computerized processes (Frey and Osborne, 2013).

ICAEW published in 2013 a report which targets the new type of information security: the cyber security. In line with the ACCA studies, the ICAEW (2013) research highlights the fact that cyber security is no longer the exclusive concern of IT departments, but has become in the last years a frequent issue within the boards of the companies, drawing the attention of the investors, which start to focus more on the aspects and incidents of information security. The study states that, until now, the financial auditors had to focus only on the accuracy of the financial data, but from now on, they also have to focus on the controls for the security of the information, which might have a significant impact on the organizations and on the financial information. In this regard, external auditors will have an extremely important role in offering assurance regarding the management of cyber risk.

The Center for Audit Quality published in 2014 an alert for the CAQ members, after SEC underlined the importance of information security. Thus, CAQ (2014 a, b) emphasized the necessity for financial auditors to understand both information systems and information security, not only of the processes and applications that might affect the financial statements, but also to obtain a general understanding of the IT systems and information security, especially when those are liable to affect the activity of the companies.

Taking into consideration that financial auditors must be capable of keeping pace with the changes in related areas, such as information technology, in the future, it is expected that professional bodies will impose a higher level of education and knowledge for financial auditors in the analysis and information technology field (Byrnes et al., 2012).

Considering all the researches presented, it can be stated the fact that at international level, there is an attempt to make the financial auditors aware of their obligations during audit missions, encouraging them to cross over the limitations of the financial accounting

field, by understanding how different factors, such as information security, might represent a core risk for the audit missions.

2. Research methodology

The purpose of this paper is to highlight if young current and future financial auditors are fully aware of the need to understand and assess information security during audit missions and the impact that the information systems' risk has on the audit risk. Furthermore, we consider to be relevant their perception regarding the mandatory skills that the financial auditors will need to have in the coming years, such as knowledge of *data mining* concepts, information security and analysis and data modelling.

As proven by the ACCA reports (2013, 2015, 2016), at the global level, there is a high degree of awareness regarding the necessity of adapting the knowledge and abilities of financial auditors to the changes from the information technology field. In this regard, the aim of this research is to investigate if in Romania, in the case of young and future financial auditors, the same level of awareness is present.

In the studies conducted by ACCA, the respondents were members of the professional body, which proves the fact that the sample was made up of participants with a high level of knowledge and practical working skills. In order to have a similar level of homogeneity in the current research, the potential respondents have been selected in order to fulfil at least one of the following conditions: to be a member of the Chamber of Financial Auditors of Romania (*Camera Auditorilor Financiari din România* – CAFR) or ACCA, to be an ACCA student or to be enrolled in the CAFR practical training program.

The current research is mixed and based on two investigation techniques: a survey and a semi-structured interview.

The survey included 12 questions and was addressed to young professionals. The majority of the respondents had an average working experience in financial audit of two and a half years. The survey was sent via e-mail to 80 persons from the groups mentioned above. Between March 25, 2016 and April 1, 2016, 25 answers were received , representing 31.25% of the selected sample. In analysing the responses there have been taken into consideration the degree of homogeneity of the community and all the questions were mandatory.

In the survey different types of questions have been used. Five points Likert scale questions (where 1 expresses a low importance/impact and 5 expresses a high importance/impact) were used due to the fact that we considered the answers to this questions to be more relevant at a more detailed level, especially because according to the specialized literature, they are more suitable in the case of perception-based studies. The survey also included single and multiple choice questions for the questions that did not need a high degree of differentiation, and ranking questions.

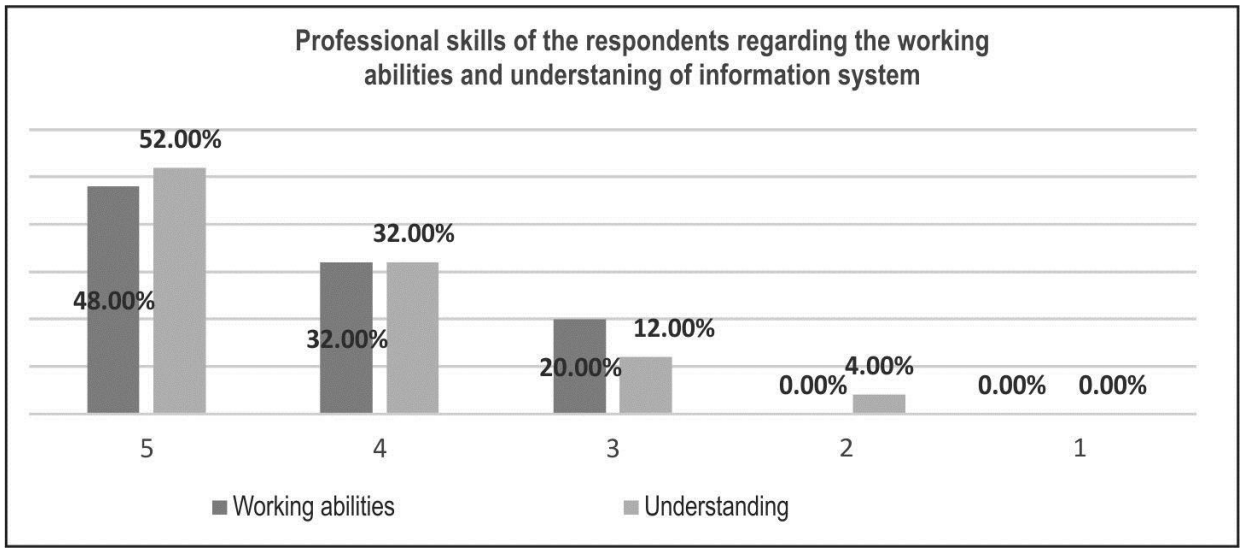
The second investigation method used for the study was the interview with five participants, which were also respondents to the survey, and are working in the audit departments of two of the Big Four companies. The scope of this interview was to assess the working procedures in audit missions of the Big Four companies. The questions focused on the way in which the financial auditors actively participate in checking and assessing the controls of the information systems and security, elements that might affect the financial data.

3. Results and discussions

Of the 25 respondents, 20 are working in the financial audit field and have an average working experience of 2.5 years. 15% of the respondents are CAFR and ACCA members, while 80% are ACCA students. Only one respondent is enrolled in the CAFR practical training program. The rest of the respondents, which are not working in the audit field, are four CAFR trainees and one ACCA student, all in the process of becoming financial auditors.

The respondents have been asked to self-assess their levels of understanding and abilities to work with information systems on a five-points Likert scale (where 1 expresses a low understanding/capacity and 5 expresses a high understanding/capacity). Taking into considerations the responses, the average score of the respondents' evaluation of their abilities was 4.2 points out of the maximum of 5 points and the average score of their evaluations regarding the understanding capacity of the information systems functionality was 4.3 points. With regard to these results, it can be stated that the participants to the survey consider having above average abilities of working with and understanding information systems.

Figure 1. Professional skills



Source: Author's processing

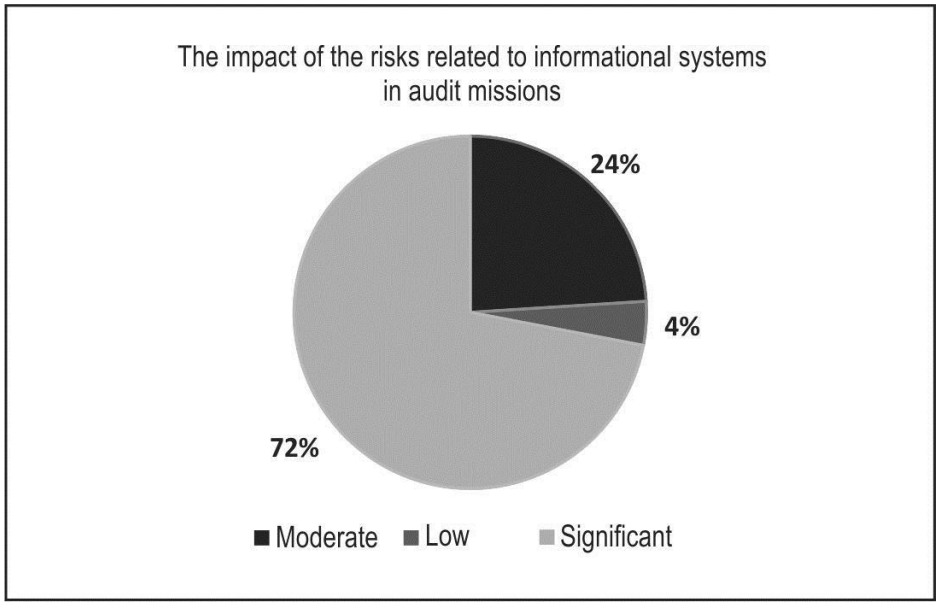
As it can be observed from the above chart, more than 80% of the respondents consider they are possessing above average skills and knowledge regarding the information systems.

In order to check if respondents have the same level of awareness regarding the impact of the IT changes on the profession, the participants have been asked to assess the impact that the information technology progress will have over the auditor's activities. At this question, the respondents were asked to choose one of the following answers: "a significant impact", "a moderate impact" and "a low impact". All the respondents considered the impact to be significant, which underlines the fact that they are aware of the impact of these progresses. Taking into consideration the studies presented above, it can be stated that no only experienced auditors understand the need to adapt to the changes from the IT field, but also the young professionals possess the same level of awareness.

Considering the structure of the sample and the fact that most of the respondents are part of generation Y, always wanting to keep up with the changes in the IT field, it follows that the participants are relying on the professional bodies to enhance their knowledge in the financial audit field. In this regard, we considered it is necessary to highlight the respondents' perceptions regarding the support offered by the professional bodies in the case of the auditors' understanding of their professional responsibilities regarding the informational systems and risks associated with information systems. At this question, only 36% of the respondents considered that the support offered is sufficient in order to understand the necessary skills needed when working with information systems and the potential risks. Meanwhile, 52% agreed with the fact that there is a support from the professional bodies, but it is insufficient, and the rest of 12% considered that there is no support offered. The variation of the answers can be justified by the fact that in the practical training programs for becoming auditor there are no specific modules which focus on the informational systems.

In the research by ACCA, ICAEW and CAQ regarding the changes in the IT field, the risk that derives from informational systems is often a key issue. Consequently, the participants have been asked to quantify the impact of the risks attached to information systems on the audit risk.

Figure 2. The impact of IT risks over financial audit



Source: Author's processing

As it can be observed, the majority of the respondents considers the impact of the risks related to information systems to have a significant influence in audit missions; there are also some variations in their perceptions, which can be explained through practical work experience.

Even though in the actual digitization era no company can be considered too small to be protected against the risk related to information systems, not all the organizations have enough resources and/or do not have a sufficient level of understanding of the need to allocate resources in order to increase the protection against IT risks. The risk associated with information systems has a more significant impact in the case of big companies, which base their operational activities on the information systems, such as financial institutions or *E-commerce* companies. For these companies, the risk related to IT systems and applications might have a significant impact.

Even though the main purpose of the questionnaire was focused on the participants' perception regarding that the current and future information security on the profession, this was not one of the first addressed questions, considering that is more efficient to switch to this key question gradually, having information systems as a general starting point.

Having as milestone the ACCA (2013) report "Digital Darwinism: thriving in the face of technology change" and three out of the ten elements that are liable to alter the financial profession, the respondents have been asked to choose from the following alternatives: "information security", "*big data*" and "*E-commerce*" or "none of the above" the one that could have the greatest impact on the profession. The majority of the participants (48%) considered that information security is more likely to influence the profession and 28% considered *E-commerce* to have a more significant impact, while the rest of 24% of the participants have chosen *big data*. The responses prove the capacity of young financial auditors to cope with the challenges caused by the progress in the IT field.

The rest of the questions from the survey were rating questions using five-points Likert scales. In this regard, we considered appropriate to present a statistical analysis of the results.

The respondents graded the impact that a series of information technology elements whose understanding is essential during audit missions, and other elements which might bring changes to the profession in the next five years, from 1 (less important) to 5 (extremely important).

Table 1. Statistical analysis of the answers provided by the respondents

Question/ Indicator	IT elements – the necessity of understanding them during audit missions			IT elements – the impact of these in audit missions		Necessary skills that the auditors must possess in the future			
	Modules of the financial applications used by the client	The functionality and flow of the applications used	Information security and related controls	Big data working skills	Information security incidents that affect the activity of the companies	The use of *data mining* techniques	The use of support applications for analysis and data modelling	Know-ledge regarding information security	Know-ledge about payment systems
Average	4.52	4.48	4.68	3.92	4.28	4.24	4.68	4.52	4.36
Standard deviation	0.64	0.64	0.61	0.84	0.66	0.81	0.47	0.64	0.79
Minimum	3	3	3	2	3	3	4	3	3
No. of min.	2	2	2	2	3	6	8	2	5
Min. frequency	0.08	0.08	0.08	0.08	0.12	0.24	0.32	0.08	0.20
Maximum	5	5	5	5	5	5	5	5	5
No. of max.	15	14	21	6	10	12	17	15	14
Max. frequency	0.60	0.56	0.84	0.24	0.4	0.48	0.68	0.60	0.56
Median	5	5	5	4	4	4	5	5	5
SKEW	-1.05	-0.90	-1.86	-0.69	-0.41	-0.50	-0.82	-1.05	-0.78

Source: Author's processing

As presented in the specialized literature, during audit missions it is not sufficient to check the accounting and fiscal accuracy of the financial information of a company, but it is also required to understand the way in which financial data is produced. In this regard, the respondents have been asked to assess the importance of understanding the following issues during audit missions: the modules of the financial applications used by the client, the functionality and data flows of the software used and also the information security with the related controls.

As it can be observed in the analysis from **Table 1**, the majority of the respondents consider that during audit missions all the presented elements must be taken into consideration, from the financial accounting applications to the data flows and the information security controls.

With regard to the modules and functionality of financial and accounting information systems and software, it is vital to understand how flows from different modules (such as the acquisitions and sales modules, productions or payments modules etc.) are producing the financial accounting data of the company, through various operational processes. Although many companies use integrated systems which include all the modules, such as ERP applications, is not uncommon the case in which a company uses different applications that are unified through specific flows into another financial application.

If in an ERP application the users do not usually change their privileges of introducing and altering data and the users' access can be easily audited, in the case in which more than one application is being used is mandatory to have similar privileges. For example, if within an information system it can be posted a record only after it has been validated by another user than the one that processed the data for the initial recording, the same level of segregation of duties must be maintained in all the other systems used by the employees, by using controls in the field of information security.

The lack of segregation of duties has a significant impact over the financial data and, in this regard, auditors should not verify only the accuracy of the financial data, but also they need to be sure that the financial information has been validated by the authorized users, maintaining in this way the integrity of the data.

The second five-point Likert scale question addressed to the respondents was focused on their perception about the potential impact of *big data* and the incidents of the information systems on the working procedures. In both cases, most participants considered that the impact is above the average. This fact is in line with the current concerns of big audit companies, which consider that *big data* allows auditors to identify more easily the frauds and the operational risks. Moreover, the incidents associated with information systems do not have to be overlooked during audit missions, even if in most of the cases they are not reported in the databases or operating systems and applications, but only in the internal network where the auditors usually do not have direct access. Due to the fact their impact is significant for some companies, the potential risks associated with information systems incidents must be taken into consideration when establishing the global risk of the company.

At the last question of the survey, the respondents have assessed the skills that an auditor should possess, in the next five years, on a five-point scale, where 1 expresses a low probability and 5 expresses a high probability. The participants have chosen between the following answers: "the use of *data mining* techniques", "the use of support applications for data analysis and modelling", "knowledge regarding information security" and "knowledge about payment systems". The majority of the participants considered there is a high probability that all the above elements will be necessary in the future during audit missions, due to the changes in the information technology field.

The answers received to this question are in line with the profession's and professional bodies' expectations. As it can be observed, the current trend is to develop new hybrid jobs within the companies, which combine the knowledge on financial reporting standards with the knowledge regarding the standards for maintaining information security.

4. Is the information security perceived properly by the financial auditors?

The above analysed survey was focused on theoretical aspects. Therefore, it does not provide the opportunity to understand what the importance of information systems and information security is during audit missions. In this regard, we considered relevant another investigation method: the interview. Some of the participants to the survey, which work in the audit departments of two Big Four companies, have been willing to present the working procedures regarding information systems and security.

It was concluded that in one of the two companies analysed based on the interviews, the members of the financial audit teams are attending IT audit training courses in order to be able to apply audit procedures and to check the controls regarding information systems. The auditors are also receiving training regarding the verification of the information security. In the case of more complex information systems, IT audit specialists are involved in specific audit missions.

In the case of the second analysed company, the members of the audit teams are not using information systems and security procedures, this task being covered exclusively by the members of the IT audit department.

In most of the cases, the changes of the audit profession start in Big Four companies, at national and international level. Therefore, we believe that in, Romania the need to develop the financial auditors' skills in the information technology field is starting to become obvious.

Conclusions

In this technology-based era, the financial auditors continue to develop new analysis and understanding skills of the companies' operational models, being capable, due to the technology, to cover wider areas of analysis during audit missions.

The conclusions of the empirical study conducted highlight that the profession is improving continuously, both in terms of specialization in the financial and accounting fields, but also in important related areas. Another key aspect is the fact that the respondents possess sufficient knowledge regarding the impact of information technology, despite the fact that the majority of the participants are not yet certified financial auditors. This is an effect of the university studies.

This paper aimed to answer the following question: "Are the young professionals working in the financial audit field fully aware of the impact that information security has on the audit missions?" We consider that through the current research we proved that the young and future financial auditors possess sufficient knowledge in the field of IT systems and security, which will be improved over time. Therefore, young professionals display the ability to analyse and assess in an objective manner the impact of information security on the organizations and by default on the audit missions, taking into consideration all the potential threats and risk areas.

The participants have proven their understanding on the fact that the profession is a continuous change and that, in the future, new skills will be required during audit missions, such as: knowing the concepts of information security, abilities of data analysis and modelling and the use of *data mining* techniques. Moreover, after assessing the working procedures regarding the information security and the analysis of the controls regarding the information systems, within the profession the necessity of having sufficient knowledge in the information technology field and practical working skills is obvious. We are taking into consideration the fact that financial auditors are trained in the IT audit and information technology area, as emphasized by the interviews.

We believe that in the near future the profession will suffer modifications due to the necessities of computerizing processes. The activities that do not require professional judgement will be automatized. Meanwhile, the financial auditors will occupy hybrid positions that will be based both on audit and information technology.

Despite the fact that young professionals have sufficient support from the professional bodies, we consider that future and current auditors need more detailed training in the information technology field, during the specialization training, but also after becoming financial auditors, due to the impact that information technology changes have on audit missions.

REFERENCES

1. ACCA (2013), *Digital Darwinism: thriving in the face of technology change*, [pdf] Available at: http://www.accaglobal.com/content/dam/acca/global/PDF-technical/futures/pol-afa-tt2.pdf [Accessed on May 7, 2016].
2. ACCA (2015), *Cyberwarriors with Calculators: The Role of Accounting and Finance Professionals in a Company's Cybersecurity*, [pdf] Available at: http://www.accaglobal.com/content/dam/ACCA_Global/Technical/tech/Cyber_threat_report_USA.pdf [Accessed on May 7, 2016].
3. ACCA (2016), *Cybersecurity - Fighting Crime's Enfant Terrible*, [pdf] Available at: http://www.futuretoday.com/content/dam/IMA/pdf/Technology/Digital/ACCA-IMA-Cybersecurity%20Report%20v8.pdf [Accessed on May 7, 2016].
4. Albu, C.N. and Toader, Ş. (2012), Bridging the gap between accounting academic research and practice: some conjectures from Romania, *Journal of Accounting and Management Information Systems*, vol. 11, no. 2, pp. 163-173.
5. Byrnes, P., Al-Awadhi, A., Gullvist, B., Brown-Liburd, H., Teeter, R., Warren, J.D. and Vasarhelyi, M. (2012), Evolution of Auditing: From the Traditional Approach to the Future Audit, ACIPA White Paper, [pdf] Available at: https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/whitepap

er_evolution-of-auditing.pdf [Accessed on May 7, 2016].

6. CAQ (2014a), *Cybersecurity and the External Audit*, [pdf] Available at: http://www.thecaq.org/docs/alerts/caqalert_2014_03.pdf?sfvrsn=2 [Accessed on May 7, 2016].
7. CAQ (2014b), *Understanding Cybersecurity and the External Audit*, [pdf] Available at: http://www.thecaq.org/docs/default-source/reports-and-publications/cybersecurity_and_external_audit_final.pdf [Accessed on May 7, 2016].
8. Chorafas, D. (2008), *IT Auditing and Sarbanes-Oxley Compliance: Key Strategies for Business Improvement*, Boston: Auerbach Publications.
9. Frey, C.B. and Osborne, M.A. (2013), *The Future of Employment: How Susceptible Are Jobs to Computerisation?*, [pdf] Available at: http://www.oxfordmartin.ox.ac.uk/downloads/academic/The_Future_of_Employment.pdf [Accessed on May 7, 2016].
10. ICAEW (2013), *Audit Insights: cybersecurity. Closing the cyber gap,* [pdf] Available at: https://www.icaew.com/~/media/corporate/files/technical/audit%20and%20assurance/audit%20insights/icaew_audit_insights_cyber_security_web.ashx [Accessed on May 7, 2016].
11. ICAEW (2015), *Auditors call for companies to recognise cyber security as a critical business risk,* [online] Available at: http://www.icaew.com/en/about-icaew/news/press-release-archive/2015-press-releases/auditors-call-for-companies-to-recognise-cyber-security-as-a-critical-business-risk [Accessed on May 7, 2016].
12. PCAOB (2010), *Auditing Standard No. 12 - Identifying and Assessing Risks of Material Misstatement*, [online] Available at: http://pcaobus.org/Standards/Auditing/Pages/Auditing_Standard_12.aspx [Accessed on May 7, 2016].
13. Stanciu, V. (2015), Considerations Regarding Financial Audit in the Big Data Era, *Audit Financiar*, vol. 13, no. 128, pp. 65-71.
14. Tudor, C.G., Gheorghe, M., Oancea, M. and Şova, R. (2013), An analysis framework for defining the required IT&C competencies for the accounting profession, *Journal of Accounting and Management Information Systems*, vol. 12, no. 4, pp. 671-696.