Faculty of Economics, University of Nis
18 October 2018

49th International Scientific Conference
QUANTITATIVE AND QUALITATIVE ANALYSIS IN ECONOMICS

ESTABLISHING AN EFFECTIVE INTERNAL IT – AUDIT FUNCTION AND CONTROL

Vesna Mladenović, MSc*

Ognjen Radović, PhD•

Abstract: *By separating the management and ownership function within the company, the conflict of interest arises. Namely, the management aims to improve the business, while the owner wants the real results and the security of the invested capital. Audit function eliminates this conflict. This paper highlights the purpose of improving the effectiveness of internal audit in the way that can provide benefits for the company according to the concept of independence and the possibilities for avoiding abuse of the audit of modern information technologies - IT audit. For developing an effective internal audit function, first of all, it is necessary to recognize its essential objective in the company. Is the auditors' goal to show how smart they are and how others in the company are dishonest, incompetent or even corrupted? The ultimate vision of IT audit is to provide the control tools to protect the information assets in the company which is most at risk.*

Keywords*: information assets, internal control, independence, risk, materiality.*

1. Introduction

When submitting the financial statements, the question of the reality of data arises, and, therefore it can endanger the interests of company's owner. As the function of company's owner and management separated, a principal-agent problem started. The conflict of interest between the management that wants to improve the company's business and the owner, who wants the results to be realistic and not to jeopardize the capital of the company, clearly outlines the need for controlling the spending of company's budget funds. This forms space for the creation of audit function and internal control. The financial reporting process itself includes an audit aimed at demonstrating an expert opinion, whether the financial statements submitted by the company's management are true and objective, and in accordance with the

* PhD student at Faculty of Economics, University of Nis, Serbia;
✉ vesna.mladenovic777@gmail.com
• Faculty of Economics, University of Nis, Serbia; ✉ ogi@eknfak.ni.ac.rs
UDC 007:004]:657.6

standards. In addition to establishing the truthfulness of the reports, todays audit function has a deeper impact on business. Namely, in modern conditions and the era of information technologies and databases that constitute the company's core resource, the audit takes on role of protecting data centers, IT control, or IT audit.

2. The definition of internal control

When defining audit and internal control, it is necessary to start from the fact that it is defined by competent professional institutions and world-famous organizations. Audit analysis is defined as the science of "discovering and analyzing patterns, identifying anomalies and extracting other useful information in the data referred to the subject of the audit and visualization regimen for the purpose of planning or conducting an audit process" (AICAP, 2015). The use of analytical tools and applications in audit process increases the quality of managerial decisions and security from risky business. By the opinion of top auditing institutions, using analytical procedures through application software not only does increase operational efficiency through cost reduction (KPMG, 2012), but also quickly identifies possibilities for fraud and anomalies, which ensures a higher level of security (EY, 2014).

The definition of internal control is formed in accordance with the basic concepts of the revision process that is being implemented and provides reasonable guarantees along with the categorization of objectives and components and criteria for effectiveness that form the framework of internal control. Internal control promotes efficiency, reduces the risk of losing information assets and helps to ensure the reliability of financial reports and compliance with laws and regulations. It can also help the company achieve its business goals and profitability and prevent the loss of resources that can provide reliable financial reporting, compliance with standards and regulations, avoiding the damage to company reputation and other consequences. In short, internal control can help the entity to get to the desired situation, while avoiding traps, surprises and risks. Unfortunately, what internal control cannot do is: a) ensure the success or survival of the company, or b) ensure the reliability of financial reporting and compliance with legal regulations and standards. The failure to observe a conceptual framework can lead to an abuse of the methodology of the audit analysis, as well as the misinterpretation of its results. In addition, many authors point out that the analytical procedure is usually used on extensive data (Schneider et al., 2015) in management, the regulators and audit participants could increase the scope of the information used, and in that way they affect the auditor's decision-making processes that provide useful information and insight into management, lawmakers, auditors and software vendors.

If we take into account previous literature in the field of analytical audit (Harrison and Datta, 2007, Kim et al., 2009, Sun, 2012), we distinguish the possibility of using analysts of audit procedures through applications from function-level capabilities. The use at the application level refers to the degree to which analysts and audit platforms are used by auditors. For example, the use of auditing data at the application level is considered adequate when using software that is often used in most audit processes.

On the other hand, future requirements related to the procedures in the revision process are a complex measure that meets specific techniques through analytical analyses (software characteristics), such as summing, regression etc. The frequency of their use depends on assuming the technological competencies, size and complexity of the company, management support, standards, and expert assistance that will have an impact on the use of analytics at the

application level. Finally, the use of analytical processes at the application level, professional assistance and technological competence have a positive impact on function level utilization, therefore, the application at both levels improves the performance of internal audit.

A recent IS research emphasizes the importance of understanding of the use of the application features of auditing software (Sun, 2012) through an organizational approach. There are studies that fill in gaps in research related to the organizational acceptance and use of technology by the auditing profession (Roi et al, 2012 Vasarhelii et al., 2012). This is due to the fact that most of the previous studies examined the acceptance and use of the tools at the individual level, not the most important participant, because the interviewing of key personnel in audit departments is difficult (Janvrin et al., 2008). So far, only a few studies have examined how audit firms or audit functions are adopting and using technology. Rosli et al. (2012) developed a theoretical model for solving factors that tried to add several organizational and external factors into their model to explore and evaluate the acceptance of application procedures by internal auditors individually and the degree to which they were adopted at the organizational level. However, it was not possible to collect actual data in order to test the proposed model and to measure the impact on external auditors using generalized audit software. The authors argued that it is necessary to examine the acceptance and use of IT at the organizational level because "the implementation of the audit technology is initiated and supported by the head of the internal audit department or higher level management (Vasarhelii et al 2012, page 18). Also, during the testing of information technology which is used in the audit domain, author Janvrin et al (2008) also pointed out that the use of the software tool does not improve the efficiency of the auditing, but its users do. The specifics for the audit software and their characteristics are defined as software tools made by the manufacturer for users with the same information technology (Sun 2012), although it is essential to separately examine the application-level usage.

Figure 1: Areas of IT Audit Management Focus

Source: (Radovanovic D., et al 2011)

Internal control is viewed as a process, and can also be viewed as a human resource. Control is not a unique event or circumstance, but a specific set of actions that permeate the company's activities. These actions are comprehensive and inherent in the way of managing and implementing a corporate strategy. They show their highest efficiency when they are

embedded in the company's infrastructure and when they are part of its core. Companies control should be "embedded" rather than "built". Internal control can be seen as a human resource. As the board of directors, management and other staff in the company execute the audit process, this aspect of auditing is also justified. The control is conducted by the people's actions and reactions in the company. People establish goals, but also control mechanisms that complete that goals.

Figure 1. describes the focus areas of management in the context of the audit process. Audit function is an integral process that connects the need to preserve the information assets with the appropriate information technology tools provided by an IT audit in conditions of high exposure to risky activities.

Also, internal control influences people's actions by recognizing what people understand, communicate or constantly coordinate. Each individual brings with him a unique background and technical capability, and each and every different needs and priorities. In order to reveal a defect in protection system of the most important data center, the company presents itself in good light at the expense of others, but if the defect still exists, this means that the company is still at risk. When the defect is removed, it means that we have actually done something that adds value to the company. Therefore, the actual mission of the Internal Audit Department is to help improve the company's state of affairs and control. By general acknowledgment, this is accomplished by performing an audit and reporting the results, but it is important to state that these actions do not provide value in themselves. They only provide value when dealing with internal control issues. The goal of the internal audit department should be to improve control and help the company solve problems in a profitable way. In short, the mission of the Internal Audit Department is twofold: first, to provide independent assurance to the Audit and Senior Management Committee that the company has internal controls and to function effectively. Improving internal controls by identifying the weaknesses of the control system and developing cost-effective solutions to address these shortcomings. (Davis C. et al 2011).

2.1. Components of internal control

Internal control consists of five interconnected components. These are derived from the way in which CEO manages business and is integrated into the management process. The components are (COSO NYC, 1992):

• Control environment. The essence of each job is its individual attributes, including integrity, ethical values and competencies and the environment in which they operate. They are the engine that company uses and the foundation on which it rests. The company's goals and the way of their achievement are based on preferences, valuations, and management styles. Often there is a compromise between competencies and costs and between the degree of supervision and the necessary level of competence of an individual. Companies can work in a formal or non-formal environment. Formal documentation is not always necessary for the effective process. A more formally managed company has the ability to rely more on written policies, performance indicators, and reports;

• Risk assessment. The entity must be aware of and address the risks to which it is exposed. It must set goals that are integrated with the company's functions, sales, production, marketing, financial and other activities to function in an integrated environment. It must also establish mechanisms for identifying, analyzing and managing

related risks. Setting goals is a prerequisite for risk assessment. Firstly, objectives must be clearly set out before management can identify steps to achieve them and risk exposure, and on that account take the necessary management actions;

• Control activities. Control policies and procedures must be established and executed to ensure that the activities identified by management are effectively carried out as necessary to eliminate the risks that limit the achievement of the company's objectives. Examples of activity control include consent, authority verification, harmonization, business review, property security and distribution of duties. Types of control activities may include preventive controls, detective controls, manual controls, computer controls. Regardless of the fact that the policy may be written, it must be applied in a planned, conscientious and consistent manner;

• Information and communication. Information and communication systems figure out these activities. They allow members of the company to capture and share the information needed to manage and control their operations. Reliable internal financial measurements are also essential for planning, budgeting, pricing, evaluating supplier performance, and evaluating joint ventures and other investments. Information can be obtained through questionnaires, interviews, market research studies on a broad scale, or targeted focus groups. Information systems must provide the right information on time and for the right place. Because of these requirements, information systems must be controlled due to their control influence;

• Monitoring. The entire process must be monitored, and the modifications must be made as required; accordingly, the system can dynamically react and change. Monitoring is not a prerequisite for internal control, because it is an essential part of it. Monitoring activities include reviews of management or supervision, comparison and harmonization. An emphasis should be placed on building rather than adding controls. Monitoring can be done in two ways: through ongoing activities or through separate evaluations. Usually, a combination of ongoing monitoring and separate evaluation will ensure that the internal control system maintains its efficiency over time.

The risks are inherent when business activities and transactions are processed by manual or in an automated way. In cases where employees deal with transactions during analysis, recording, approval, classification, processing, accounting, publishing and reporting, intentional or unintentional errors, omissions, and irregularities (e.g. theft, fraud) occur. These risks are potentially damaging events that can produce losses. High risk areas should have a high priority, and low risk areas have a low priority. A systematic approach to risk assessment is better than random access and error.

2.2. The concept of independence

The great myth of independence is one of the basic principles of the audit department. It is also one of the biggest excuses that the auditors use to avoid the requirement to create an effective control function. Therefore, as one of the key success factors that almost all audit departments emphasize is their independence and the reason why the company's management can rely on them. What is actually independence? There is much to write about independence, but the function of internal audit is not really independent. However, the essential concept behind the idea of an independent auditor is valid and very important. Defining the word "independent" implies the following description - "not to be influenced or controlled by others

in the company, to think and act on its own". This definition fits very well into the concept of many audit departments. If an IT auditor intends to work in the IT sector of the organization, it is probably the best that the director of the IT department does not consider him an employee under the influence of others. The auditor should not feel pressure to conceal problems and must be able to have a way to do the right thing. This is the moment when the relationship with the manager comes to expression.

Since the auditors, at least partially, report to the Chairman of the Audit Committee, they, therefore, consider that they are not influenced or controlled by others. If this is analyzed a bit closer, it is true that the auditor reports to a board member. However, in almost every company, the Audit Director also submits reports to the financial, general manager of the company. In most cases, the Audit Department's budget and, more importantly, employees of the Audit Department, are controlled by this managing director. It is difficult to understand how a particular person may feel that it is not influenced by other individuals (executive directors). In addition, internal auditors generally work in the same building just like all other employees involved in acquiring shares and distributing results, as well as their colleagues from other departments and it is inevitable to have relations with the employees of the audit firm.

It seems that "objective" may be a more appropriate word for describing an internal auditor than the word "independent". However, someone who is objective is not influenced by personal feelings or prejudices; he is impartial. Although an internal auditor, by some experience, is not really independent, it is fair to expect it to be objective. If an adequate auditor is engaged, they will have the ability and the will to ignore their personal interests during the audit and to observe things in an impartial manner. In order to increase their efficiency, internal auditors should take advantage of this lack of independence.

Instead of pretending not to be part of the system, they should use the fact that they are involved in the company's business. It is not possible for an external auditing firm to obtain such comprehensive knowledge of the company's operations during the audit as it can adequately form an internal audit department. Unless it is a part of the company's affairs and without the engagement of an auditor with prior knowledge of the company's operations and activities, it is wrong to make a decision to engage someone who is not the company’s employee. The fact that the company has employees from its staff as an internal auditor represents a competitive advantage. Otherwise, the function of the audit is one of the costs, and if the management can perform this function at lower costs through another service provider, it will do the same. Troubleshooting and adding controls after implementation are significantly higher than the cost when done right at the beginning. In terms of independence, there is no difference between evaluating a system, or providing a solution before implementation and evaluating it after implementation. However, there is a difference in how much additional value an auditor creates for the company. There is more in being auditor than just auditing.

The quality of internal control requires that they have to be established from the outset. Unfortunately, many auditors use independence as an excuse to avoid the requirement to create additional value and not give opinions. The auditor can always be independent and work together with colleagues to help them develop a solution to the problem of intent control. To be independent does not mean that an auditor cannot estimate the control within the system before the start of use. In many cases, it can be seen that internal audit departments refuse to give instructions and information to teams developing

new systems or processes. It is considered that auditors cannot provide information about controls within the system because it would mean that they are no longer independent. The question arises: How to conduct an audit in the company where the same staff has already approved the control system? If bad control is conducted before the implementation of the control strategy, then auditors are equally responsible for the failure of controls, as well as the IT team that has a higher system implementation. Auditors should make a step forward and provide information. Whether an opinion is formed before or after the implementation, however, it is smart to provide essentially the same information. Namely, how can the information given this week damage your independence, while the information given next week (after implementation) would not hurt? There is disagreement in this. The key question that often arises relates to the future independence (or objectivity) of the auditor who performed the initial consulting.

Will the IT be allowed to audit the system in the future? Or, whether they are compromised by the fact that they have already approved the control system and do not want to distort their reputation by admitting that they have missed something. That, of course, is worth considering. However, we all have the right to know new facts over time, "we become smarter" and not apologize if the results of the audit after the implementation reveal the existence of a problem that we did not take into account before the implementation. An auditor who was engaged before the implementation would be the most common resource for auditing after implementation. It's a shame not to take advantage of that potential. As noted earlier, the audit objective is to improve internal controls. Who is more suitable for carrying out a detailed audit if not the person who is a member of the team working at the same time from the start? If there is still a concern about the auditor's objectivity, the auditor may be considered a member of the team, but not a team leader. In this way, a special level of control of the auditor's work is ensured and can be proved that they are not under the exaggerated influence of their previous work. The auditor should usually be involved in the team as an advisor. The auditor cannot perform the controls and review them, but should be free to provide as much information as possible about how the control should look. Each information system has its own life cycle, because each system appears at a given moment, then develops and disappears after a certain time, it is replaced by another. When talking about the life cycle of the information system, then we can say that it has four phases, and they are (Panian Z, 2001):

- The initialization phase - at this stage, the company's management points to the need for the development of the information system, and together with the discussion and suggestions, the system is being prepared;
- Stage of expansion - after a certain time, resources, knowledge and efforts are invested in the process of expansion or growth. At this stage, the equipment is being prepared, staff training is being carried out, as well as the networking of the system;
- Consolidation phase - known as the phase of system maturation, where the system achieves a certain criterion in terms of quality, efficiency and effectiveness;
- The fourth stage of maturity of the system - at this stage, the information system user begins to receive the necessary information, and the goal is to keep the system as long as possible at this stage in order to pay the company's investment.

The core of the information system today is a computer. The task is to process data and form information with its software performance, which will enable the management to make important decisions more easily. Today, the computer has a low price that can be

afforded not only by companies, but also by individuals, and its value is multiplying. The focus is on data processing equipment, which ultimately leads to a fundamental and everyday control and audit of the information system.

The only reasons why the revision of the information system is of crucial importance and which Zeljko Panijan discussed in his book are (Panian Z. et al, 2006):

- Data loss costs - data represent the basic resource of each company, and we obtain important information from the data by special processing. However, in case of loss and damage to the data center, the company does not have the necessary information and can lead to significant losses of information assets. For these reasons, it is necessary to constantly monitor the work of computers in the information system;
- The cost of making inappropriate or wrong decisions - the quality of decision-making is of key importance to the quality of data and decision-making;
- Costs of misuse of IT equipment - the main reason for control and audit of the IS is the misuse of IT equipment. The way in which the equipment can be misused is, for example, attack by hackers, various dangerous viruses, theft, etc.;
- Value of equipment, programs and employees - data are considered a critical resource of the information system in combination with hardware (software), software (program) and live program (users). Today, the value of equipment and software is decreasing, but the value of IT professionals who maintain it is on the rise, as more and more users have demands for experts. The loss of equipment, as well as the destruction of a program, can lead the company to the brink of collapse, as the business would be partially or completely disabled, which requires huge unnecessary costs;
- Computer error costs - today computers replace some of the jobs previously performed by people, and for these reasons their control and revision are necessary not to make mistakes that can be a matter of life and death;
- Preservation of privacy - all information that the company owns, even those about clients must be protected, because they can be misused by individuals. For these reasons, the social community should, with the help of its administrative authorities, adopt legislation to protect the privacy of individuals;
- Controlled improvement in the use of IT equipment - as mentioned earlier, the information system is experiencing its growth in the expansion phase, where unexpected activities can occur which are eliminated during the consolidation phase. Further investments and system upgrades should continue beyond the final phases of the life cycle of the information system.

Defining the concept of the audit of the information system according to Miroslav Hadzic, the term revision of information systems means the collection and evaluation of evidence from which it can be realized that the preservation of information in an appropriate manner, data, allows you to examine the effectiveness of achieving set goals, and whether you are using efficiently available resources. (Hadzic M., Radoman J., 2009)

From this we can conclude that the task of revision of information systems is:

- To provide better protection of the assets of the company's information system - The assets of the information system of the company include hardware, software, digital knowledge, system documentation, as well as auxiliary equipment and materials;

- To achieve a higher level of data integrity - when it comes to information system revision, this term examines the degree to which the data is characterized by the necessary attributes: completeness, clarity, purity and truthfulness;
- To promote system efficiency - when we talk about the efficiency of the system, and in relation to the audit of information systems, relate to the ability of the system to achieve the set goals. Promoting the efficiency of the system means that it uses the least possible resources to achieve the set goals.

2.3. Materiality planning

Factors that influence audit testing:

- Materiality;
- Audit risk;
- Business risk;
- Cost and time.

Materiality is defined as the size of the wrong assessment that would affect the judgment of a reasonable user of the financial statements. Material errors, irregularities and illegal actions will have a direct impact and material effect on the value of the financial statements. From the IT audit point of view, materiality refers not only to the financial statements, but also to the business and information systems. From the financial statement's point of view, materiality is assessed against the financial statements as a whole. From the operational point of view, materiality should be assessed in relation to the particular operation being considered, as well as to all other operations to which it relates. From the point of view of the information system, the materiality needs to be assessed in relation to the particular information system being considered, as well as all the other systems of connection that relate to it. Weaknesses in materiality in business operations or in computer systems may or may not have a direct impact on the financial statements. For example, the continued use of pirated software can become a sensitive and material issue if it was known to software vendors or other interested third parties who are there to monitor the situation of software piracy in companies. This is because the penalties could be high, and the purchase of software through official sources would cost more. In addition, the loss of reputation and bad reputation is a major factor in thinking.

Similarly, unauthorized expansion of production formulas, knowledge of processes and disclosure of secret recipes to competitors would have a material effect when a competitor decides to use new information. Another example is the impact of poor quality products and possible environmental damage on the part of the organization. Weaknesses in materiality in business and in computer systems reflect business risk. It is the risk of negative advertising and a permanent damage to the reputation of the organization that is crucial. Business risk (exposure risk) differs from the audit risk. The audit risk, from the IT auditor's perspective, is best defined as the risk that the auditor cannot reveal a significant error or weakness during review and audit. Who should set the level of materiality? The auditor and the IT audit department should understand the levels of materiality and the level of security that are applied in the audit. This understanding should be based on the confrontation of costs and benefits. The auditor's decision plays an important role in determining the materiality and amount of audit work being done, as well as in assessing the evidence being collected. Providing formal guidelines for auditors can increase consensus.

What is material and immaterial? As the professional practice requires, the auditor has to consider the relative materiality or significance of the issues to which the audit procedures apply. Various studies suggest that the size of the error as a percentage of income is the most important factor in determining its significance. Items that have an effect on income greater than 10% are normally considered material, while the items that make up less than five percent of income would normally be considered irrelevant. The auditor would most likely assess the error in the income statement as material, if the error involves a large percentage of net income. Most likely they are material: (1) trivial mistakes that are unlikely to happen again, (2) unverified routine transactions, or (3) unusual transactions for the company. When an affiliate is involved, such as a major shareholder, the error would be considered material when the balance sheet of the shareholders' claims amounted to less than one percent of the company's claims. Other materiality factors, in addition to the income effects, include the effect on the earnings trend, the effect on working capital and the effect on total assets. Legal and political factors are important, and respect for laws and regulations is also crucial. As a practical matter, the level of security cannot be separated from materiality. Considering the same sample size, the auditor with a lower level of materiality will have a higher level of auditing risk; the auditor's risk would be comparable between the auditors, the level of security must be related to the level of materiality.

2.3.1. Qualitative and quantitative materiality

Sometimes the nature of detection (sensitive or not) and evidence of the desire to detect an error (by accident or intention) is more important than quantitative factors. The auditor needs to behave more towards human behavior. Quantitative materiality is applied in the audit planning phase. Qualitative materiality is applied during the audit assessment phase, because it is not practical to plan the audit to uncover qualitative misstatements. How to calculate materiality? Materiality is calculated by taking the base and multiplying by a percentage. The database, in descending order of importance, includes total revenues, total costs, total assets, retained earnings, and revenues. The percentage used can be equal to a percentage or one obtained from a slip scale. The final percentage is based on the notion that materiality is completely relative, while the scale is based on the belief that some quantities are large enough to be always material. A survey by government auditors noted that most (65%) respondents use a fixed percentage, and 35% use scale scales to calculate materiality. The audit revision has three components: inherent risk, control risk and detection risk.

Its relation to other types of risk is described below:

Audit risk = inherent risk * control risk * detection risk

Audit risk is the risk that the auditor can unconsciously change his opinion on the financial statements that are materially misstated. The inherent risk is the sensitivity of the claim to a material misstatement, assuming there is no structural policy or procedure. Control risk is the risk of material misstatement that may arise in the assertion that it will not be timely prevented or disclosed by the policies or procedures of internal control of the entity. The risk of detection is the risk that the auditor will not detect the material misstatement that exists in the claim.

The American Institute of Certified Public Accountants (AICPA) defines the audit risk as being likely to give an unqualified (pure) opinion on the financial statements actually

contain material misstatement. The risk of an audit is, therefore, a complement of the level of insurance; which is the lower risk of revision, the greater the guarantee, and vice versa. Since audits are performed on the basis of a test or sample, the audit risk cannot be reduced to zero, except for overheads. This is because even small reductions in materiality and/or auditing risk can result in a disproportionately large increase in the sample size and hence audit costs. During 100% verification, the audit risk cannot be reduced to zero. About 53% of respondents in the auditor's research have stated that they usually try to quantify the audit risk in determining the scope of audit testing. The risk and materiality of the audit are important reasons in planning the audit process and evaluating the final results. Materiality plays a major role in planning the scope of audit and the scope of audit testing, as well as in assessing the adequacy of audit evidence (S. Rao Vallabhaneni, 1996).

In order to audit information systems, a wide knowledge of information technologies is necessary. Some special skills are needed:

- Understanding the function, expectations and overall performance of the information system in the audit, project management and software;
- Using CAAT (computer tools for auditing) tools and techniques;
- The auditor must be able to assess what are the private and security issues that can bring the company's risk,
- Evolution of the life cycle of information systems development (SDLC);
- Development of new techniques involving rapid system development and system prototyping,
- Implement a risk-oriented approach;
- Review and verify information technology companies on the basis of legal issues;
- Implement national and international standards such as ISO 9000/3, ISO 27001, ISO 27002;
- Create reports and perform audits to ensure that they work in the right way.

3. Conclusion

The information system passed through a dynamic path of development and improvement in a short period of time. Initially, the audit process of financial statements was supported, but in modern conditions, the auditing of information systems increasingly becomes an indispensable element in the process of analytical management of information technology and the links between management and IT sector. The operation of the information system is in the function of maintaining the integrity and integrity of data, as well as using the resources of the system in an effective and efficient way. The audit assesses whether information technology works in accordance with business goals, to what extent is it effective and expedient to support business objectives and what is the practice (maturity) of management and control of the information system at various hierarchical levels. IT audit, in addition to its concise and analytical function, has an advisory role and helps in corporate IT management. The auditor determines whether the information technologies are operating in accordance with the goals of the organization, and to what extent they effectively support the business goals. The economic strength of the company depends directly on the introduction of new technologies, and, therefore, on the effective implementation of the IT audit strategy.

References

American Institute of Certified Public Accountants (AICAP), 2015. Audit Analytics and Continuous Audit: Looking Toward the Future;

EY, 2014. Big Risks Require Big Data Thinking – Global Forensic Data Analytics Survey 2014;

KPMG, 2012. Leveraging Data Analytics and Continuous Auditing Processes for Improved Audit Planning, Effectiveness and Efficiency;

Schneider G., Dai J., Janvrin, D., Ajayi, K. Raschke, R.L., 2015. Infer, predict, and assure: accounting opportunities in data analytics. Account.Horiz.29 (3) 719-742;

Harrison M.J., Datta P., 2007. An Empirical Assessment of User Perceptions of Feature versus Application-Level Usage. Commun. Assoc. Inf. Syst. 20(1) 21.

Kim, H. J., Mannino, M., & Nieschwietz, R. J. (2009). Information technology acceptance in the internal audit profession: Impact of technology features and complexity. International Journal of Accounting Information Systems, 10(4), 214-228;

Sun H., 2012. Understanding User Revisions When Using Information System Features: Adaptive System Use and Triggers. Manag. Inf. Syst. Q.36 (2), 453-478;

Rosli, K., Yeow, P.H., Siew. E.G., 2012. Factors Influencing Audit Technology Acceptance by Audit Firms: A New I-TOE Adoption Framework. J. Account. Horiz. 29 (3), 719-742;

Vasarhelii M.A., Alles. M.G., Kuenkaiaew, S., Littley J. 2012. The acceptance and adoption of continuous auditing by internal auditors: A micro analysis. Int. J., Account. Int. Syst.13 (3), 267-281;

Janvrin, D., Bierstaker, J., Lowe, D.J., 2008. An Examination of Audit Information Technology Use and Perceived Importance. Accounting Horizons: March 2008, Vol. 22, (1) 1-21.

S. Rao Vallabhaneni. *CISA examination textbooks: Theory, Volume 1*. Front Cover. SRV Professional Publications, 1996;

Radovanovic D., Sarac M., Adamovic S., Lucis D., *Necessity of IT Service Management and IT Governance*. IEEE, MIPRO 2011- DE, May 23-27, Opatija, Croatia, ISSN 1847-3938, p. 84-87.

Davis C., Schiller M., Wheeler K. *Auditing of information technologies – use of controls for protection of information assets*. SRRS 2011;

The Committee of Sponsoring Organizations, *Risk management in enterprises, Integrated framework.* COSO, NYC, 1992;

Panian Z. *Control and audit of information systems*. Zagreb, 2001;

Panian Z., Spremic M. and co. *Corporate management and revision of information systems.* Tiskara Zelina, Zagreb 2007;

Hadzic M., Radoman J. *ECONOMY and security* Vol.1. – Belgrade: Center for Civil-Military Relations, 2009.

USPOSTAVLJANJE EFEKTIVNE INTERNE FUNKCIJE IT - REVIZIJA I KONTROLA

***Rezime**: Razdvajanjem funkcije upravljanja i vlasništva unutar kompanije, dolazi do sukoba interesa. Naime, menadžment teži poboljšanju poslovanja, a vlasnik želi da rezultati budu stvarni i da ne ugrožavaju uloženi kapital. Ovaj sukob pokušava da eliminiše funkcija revizije. U radu će se razmatrati svrha interne revizije i način na koji se ona može najbolje iskoristiti za obezbeđivanje koristi za kompaniju. U skladu sa konceptom nezavisnosti i mogućnostima za izbegavanje zloupotrebe, ističe se način poboljšanja efektivnosti revizorske funkcije i uloga revizije savremenih informacionih tehnologija – IT revizije. Razvijanjem efektivne funkcije interne revizije, potrebno je pre svega spoznati suštinski cilj iste u kompaniji. Da li je svrha objavljivanje izveštaj, ili je cilj da revizori pokažu koliko su pametni i koliko su ostali u kompaniji nepošteni, nestručni ili čak korumpirani? Konačna vizija jeste da IT revizija obezbedi alate za kontrolu radi zaštite materijalno značajne informacione imovine i centra podataka u dobu kada je kompanija najviše izložena riziku.*

***Ključne reči:** informaciona imovina, interna kontrola, nezavisnost, rizik, materijalnost.*