Stanislav Mitrović

The Methodological Aspects of Information Technology Risk Identification in Internal Audits

Article Info:

Received 18 October 2014
Accepted 12 December 2014

UDC 004:005.334

Recommended citation:

Mitrović, S. (2014). The Methodological Aspects of Information Technology Risk Identification in Internal Audits. *International Scientific Journal of Management Information Systems, 9* (4), 15-23.

Summary

The article looks into the methodological aspects for risk assessment in the area of information technology application (IT risk), performed for internal audits purposes. The author analyses the current state in terms of methods for assessing risk and its components, and the systematization of the basic factors affecting risk assessment. Particular attention is devoted to the analysis of normative and methodological documents dealing with the risk identification issue in the areas of application and use of information technologies in organization. Elaboration of models for the practical assessment of IT risk, within a more broadly viewed concept of risk assessment for the needs of internal audit, was performed on the example of control self-assessment, whose theoretical foundations are currently still in the initial stage of formation, which contributes to the relevance of the topic and provides a basis for further research into the observed problem in perspective.

The essential conclusions of this paper confirm the advantages and point to the necessity of integrating competencies in the area of auditing and knowledge in the area of information systems. Comprehending the influence of information technologies on the audit process is established as one of the key competencies, which is not only desirable, but also indispensable for all internal auditors involved in the problems of organizational risk assessment and management.

Keywords

internal audit, risk, information technologies, self-assessment

1. Introduction

In the opinion of many researchers, the theory of risk, whose components were deeply and scientifically elaborated in the 1980s and '90s, remains one of the most problematic areas of auditing. This situation is related to the fact that many experts continued interpreting the term "risk" in different ways, in different specialised areas and scientific schools, which is reciprocally reflected on determining the methodological approach to its measurement.

The economic reforms conducted in many countries worldwide in the late 20th and early 21st century, and continued development of the global financial crisis, several waves of which made a significant impact on the world economy, compelled the managers and owners of companies in different countries to strengthen the role of internal audit as an inseparable component of the corporate management system, which is directly related to improvement in business efficiency. Thus, for instance, the Sarbanes-Oxley Act of 2002 adopted in the USA, has become the main regulating document in the given area, and although it is primarily related to the obligations of public companies, it affected significantly the development of internal audit and control, and also the development of the theory of risk and risk assessment, not only among the American academics and practitioners, but in the entire practice worldwide. The internal audit's obligation to deal with risk assessment issues and enhancing companies' risk management process also stems directly from the Internal Audit Standards, issued by the Institute of Internal Auditors (IIA). So, for instance, standard 2120, pertaining to risk management, unequivocally states that the internal audit is to provide an assessment of risk exposure, related to managing, operation and information systems, in connection with reliability of financial reports, efficiency of operations, efficiency of operations, protection of property and compliance with laws and regulations, and also the company's policies, procedures and standards.

After the adoption of the International Standards on Auditing (ISA), the concept of auditing was substantially expanded and is no longer limited to checking accounting records and tax returns of the audited entity. Audit has become a multi-profiled activity, and nowadays includes analysing financial activities, studying the internal control systems, assessing risks related to the application of information technologies, analysis of risks and their influence of financial reporting, etc. Such expansion resulted in the need for constant advancement of auditors' qualifications, acquiring

and exchanging new knowledge and practical experience, for developing new methodological tools with the aim of discovering actual theoretical and practical problems and possibilities for their resolution.

This trend of extending the role of internal audit is also confirmed by the results of an international research projects by the PricewaterhouseCoopers (PwC) (2009), showing that, in the foreseeable future, internal audits are planning to pay more attention primarily to IT risks (83% respondents); then operating risks (81%) and other business-related risks that occur (78%). In addition, the traditional field of activity of internal audit – (controlling compliance with regulatory criteria and policies) – will also remain priority in the forthcoming years, despite the lowest degree of impact on the company's shareholder value.

2. Systematisation of the basic factors affecting the risk assessment

When appearing on the global, national or local market, every company's primary goal is to create stakeholder value for those involved in its activities. In such circumstances, organisations are, first of all, faced with uncertainty, and, in connection with this, the task of managing bodies is to make a joint decision on the degree of uncertainty that the company is willing to accept in its effort to increase stakeholder value. In this case, uncertainty includes two opposing features – the existing risk on the one hand, and opening prospects, resulting in value decrease or increase.

The existence of risk is directly related to the reverse side of economic freedom. Freedom on the economic market is provided for all entities of economic activity; the freedom of one entity is accompanied by the freedom of other suppliers and consumers, so that uncertainty and risk grow with the development of market relations.

As the analysis performed within this research, the contemporary academic literature often does not distinguish between the terms "risk" and "uncertainty". Yet, there is a significant difference between the two, especially in relation to internal audit: risk characterises a situation where the emergence of unknown events is highly likely and can be assessed in terms of quantity. Uncertainty is a broader and more encompassing notion, as this phenomenon is caused by all factors affecting the final result of economic activity; it is characterised by the fact that it is impossible to foresee the likelihood of emergence of unknown events.

Despite the paradox, which is obvious at first sight, uncertainty contains the primary level of managing a company's operation. Risks occurring at the moment of creating the company remain the key motivation and offer the company's management the possibility to establish the strategy and tactics of the organisation's functioning. Risk management enables efficient functioning in the conditions of uncertainty and risks related to them, and exploiting opportunities, thus increasing the potential for the growth in the company's value.

In their work, companies face both internal and external risks of the widest range, including the constant grow in the risk of various abuses. The analysis of information from sources systematising the basic aspects of the research problem (e.g. Knight 1921, Bernoulli 1954, Brown & Solomon 1990) enables the classification of external factors affecting the degree of risk and its assessment as follows:

1. Factors of direct impact, which directly affect the results of economic activity; these include:
   - legislation and standards regulating economic activity,
   - actions of public services and institutions
   - taxation system,
   - relationships with partners,
   - competitors' activities, and
   - corruption.
2. Factors of indirect impact; these cannot affect the risk directly, but contribute to its change:
   - political conditions,
   - economic situation in the country,
   - the company's economic position on the market, and
   - Force Majeure.

Internal factors include: the organisation's strategy, managing and decision-making model, organisation of purchase and sale processes, availability of financial assets, likelihood of embezzlement by employees, the staff's qualifications, likelihood of discontinuing business activities etc.

In addition, one of the important risk factors faced by companies is related to the application and use of information technologies in the organisation's business (hereinafter referred to as IT risk). The impact of this factor is highly complex and specific in contemporary conditions, which is why it is hard to classify it into one of the existing above mentioned categories. Risks in the application of information technologies can be both internal and external, with direct and indirect

impact on business results, and furthermore, they can be related to legislation, the economic situation in the country, the staff's qualifications, availability of financial assets etc. For this reason, risks related to the application of information technologies are viewed as a complex category with an extremely large potential negative impact on organisations" operations, whose assessment should take up a special place within the broader concept of risk identification and management in internal audits.

3. Methodological approaches to risk assessment in international practices

Events happening worldwide lately show that scientific and business groups making decisions based on risk assessment are still facing difficulties in the area of risk management, and the methods applied for their assessment. On the one hand, the cause of this is the complexity of the risk assessment process, and on the other, loss of confidence in existing methodological solutions, as the consequences of the latest global financial crises in the first decade of the 21st century, whose waves are still obstructing the work of economic entities, have shown that risk assessment instruments most frequently applied in organisations are obviously insufficiently scientifically elaborated and insufficiently efficient, or unsuccessful in the specific conditions in the capacity of tools for preventing risky situations.

In fact, nowadays there is an imbalance between the expectations and results of the application of methodological instruments, which is mostly explained by vagueness and complexity that one has to face when assessing risks (PWC Internal Audit 2012: 8). Starting from this assumption, scientific organisations, individual researchers, and also international regulators are currently undertaking multiple activities aimed at increasing the degree of objectivity and transparency of toolkits used in risk assessment, for which reason, based on contemporary knowledge, more advanced methodologies are developed, enabling increases in quality, reliability and operability of solutions and undertaken actions in terms of risk assessment.

It must be pointed out that, within contemporary approaches to risk assessment in organisations, the risk factor is not considered within a unique methodological approach, which additionally influences the variety of assessment methods for this economic category. Before we proceed to a more detailed analysis, we shall pause briefly to interpret the definitions of the terms "methodology" and "method", and express precisely the sense they are given in this research. In our paper, we rely on understanding methodology as a set of existing goals, tasks, forms, methodological approaches and methodological toolkit, forming the method of an organisation's risk assessment, and the teaching on the risk assessment system itself. Thus, risk management methodology and method (application of models, forms, methods and other instruments) stand in a relationship of a section and the whole, where the latter concept represents a part of the first.

The analysis of international practices in the organisation of internal audit shows that, when assessing risk in their professional area, internal audit services and their co-workers are predominantly led by internal documents, whose provisions are formulated in compliance with international criteria, presented in the Code of Professional Ethics for Internal Auditors, adopted by the USA Institute of Internal Auditors (IIA), and The International Standards for the Professional Practice of Internal Auditing (IIA Standards 2013).

We must point out the fact that international standards should still be understood as general instructions or the starting point for developing internal standards for internal audit activities, establishing unified criteria for carrying out audits, disclosure of results of auditing and consulting services, for the procedure of preparing final documents, for preparing, retraining and increasing the qualifications of internal auditors in every economic entity (IIA Standards 2013: Intrd. 2). As shown by the analysis of international practices in the operation of economic organisations, methodological reliance of risk assessment activities solely on international standards is not sufficient. In relation with this, it is useful, as a supplement to internal audit standards, to develop applications and methods for checking various objects, worksheets, document forms and other types of business documents, which will enable a complex approach to audits and increase objectivity in risk assessment.

When considering risk assessment methodology, it is important to point to the fact that every audit begins by setting criteria. Planning risk assessment activities related to the application of information technologies, an internal auditor is obliged to take into account the risk management concept adopted within the organisation, including the implementation of maximum-level risk established by the executive management for different types of activities or organisational

segments. If the existing assessment criteria are appropriate, the internal audit uses them as guidelines and benchmarks. If the case is the opposite, the internal audit and the organisation's management set assessment criteria based on advanced methodologies, applicable in specific cases, and relevant technological patterns (the best practice), which enable the organisation to perfect the processes up to the level that is above average in its area. Consequently, the internal audit is oriented to yielding benefits and creating value added for the organisation also in the part of activities related to analysing IT risk from the very beginning.

4. Comparative analysis of the methodological basis for identifying IT risks in internal audit

The methods and models of risk identification, present in practice within the realisation of the goals of internal audit, stand in direct correlation with the relevant normative and methodological basis in the area of risk management (Colbert, Bowen 1996: 27). Normative and methodological document are used in contemporary conditions when assessing and consulting in the area of risk management systems, and can be classified into three basic groups:

- concepts, which are comprehensive for organisations in different areas,
- the regulators' normative documents, and
- recommendations by specialised, expert organisations and practices f leading companies in the leading area.

Various international organisations have developed a whole range of standards or regulatory frameworks, enabling the assessments of various aspects of the internal control system. Among the most significant and established normative and methodological documents in international practice dealing with the issues of risk in the area of information technology application indirectly or directly, the most prominent are COBIT, SAC, COSO and SAS 55/78:

1. The standard Control Objectives for Information and Related Technology - COBIT 1996, compiled by the Information Systems Audit and Control Foundation's Control Objectives for Information and Related Technology (ISACA);
2. The report System Control and Audit (SAC 1991, revsd. 1994), compiled by the Institute of Internal Auditors Research Foundation's Systems Auditability and Control;
3. The report Internal Control: the Integrated approach (COSO 19921), compiled by the Committee of Sponsoring Organizations of the Treadway Commission's Internal Control – Integrated Framework;
4. Instruction for revising the structure of internal control structure when auditing financial reports (SAS 55, 1986), established by the American Institute of Certified Public Accountants' Consideration of the Internal Control Structure in a Financial Statement Audit, with amendments (SAS 78, 1995).

We shall elaborate on each of the above listed documents.

The COBIT (1996) Standard updated on a systematic basis the definition of control, set in the COSO Report, including the norms, procedures, techniques and organisational structures that had been developed to provide a reasonable guarantee that business objectives would be achieved, and unwanted events prevented or detected and rectified.

COBIT adapts the definition of IT control, taken over from the SAC document, and represents the declaration of the desired result or goal, which is to be achieved by implementing control procedures in a certain IT activity. COBIT highlights the role and influence of IT control, pertaining to business processes, and defines the field of application of the independent goals of IT control. This document classifies controlled and controlling IT resources to data, application systems, technologies, technical tools and people. Data are defined in their broadest sense and include not only numbers, text and dates, but other object as well. Application systems refer to a complex of manual automatic procedures. Technology includes hardware, operative systems, and network equipment. Technical tools are resources used for accommodating and supporting information systems. The "people" resource refers to individual skills and abilities of planning, organising, acquiring, supplying, supporting and controlling information systems and services.

To be harmonised with business objectives, information must meet certain criteria, which COBIT sets as criterion for information. COBIT unifies principles from already existing models into three broad categories: quality, responsibility of authorised persons and safety. Out of these broad criteria, seven intersecting categories of criteria are selected to assess to what degree IT resources

match the criteria for information. These criteria include efficiency, relevance, confidentiality, integrity, availability, legality and reliability of information.

Based on the analysis of the best experiences in IT management, this standard divides IT processes into 4 zones. These zones include: (1) planning and organisation, (2) procurement and implementation, (3) supply and support, and (4) monitoring. The usual grouping of processes by zones often entails zones of responsibility in the organisational structure or follows the management cycle or life cycle, which is applicable to IT processes in any IT environment. Connection between IT resources and four IT zones is presented with examples, listing 32 individual processes in 4 zones.

COBIT is a control structure for the business process owner. Furthermore, according to the document, the management is assigned full responsibility and authority related to organisation management. The standards includes the definition of both terms, both internal control and aims of IT control, 4 process zones, 32 most important control rules for these processes, 271 aims of control, which is directed at those 32 processes, and instructions for auditors, which are related to control objectives.

COBIT's structure provides the most significant rules for specific IT processes. Document scheme defines the task, which is accomplished using audit controls, and IT resources, used for managing processes; it formulates possible audit tools and the list of the most significant audit tools and the list of the most significant audit objectives for the specific case.

The report entitled System Audit and Control (SAC) (1991, revised 1994) offers methodological support to the activity of internal auditors in the area of control and audit of information systems and technologies, and is also based on a systematic approach as the basic element. SAC (1991, revsd.1994) defines the system of internal control as a complex of processes, functions, activities, subsystems and people, unified or deliberately separated, with a task to secure efficient accomplishment of goals and tasks.

The report also points out the role and impact of computerised information systems on the area of internal audit, emphasising the necessity of risk assessment, cost and result comparison, and also the necessity of integration of the control tools into systems instead of adding them after the implementation of the system.

The SAC standard separates three key components in the internal control system structure, including: control environment, manual and automatic systems, and control procedures. The control environment encompasses organisational structure, control structure, norms and procedures, and external impacts. Automatic systems consist of the system and applicative software. When analysing the content of the document, it must be pointed out that SAC influences control risks, which are connected to the end user and systems of individual organisational segments. But does not describe and give the definition of manual systems. Control procedures consist of general, applied and compensatory control tools.

SAC represents five classification schemes for internal control tools in information systems: (1) preliminary, current and forthcoming, (2) systematic and discretional, individually initiated and prescribed, (4) manual and automatic, (4) applied and general control tools. These schemes are focussed on subject-object, temporary and aspects of other types, among others, when the control tool was deployed, whether it can be bypassed, who insists on the necessity of carrying out the control, how the control is realised, and where in the software the given control tool was implemented.

The notion of risks, defined in the content of System Control and Audit (SAC 1991, revised 1994), which we are analysing, includes abuses, errors, discontinuation of activities, unproductive and inefficient use of tools. The goals of control generalise these risks and provide an informational unity, reliability and compliance with the prescribed requirements. The content of obligations of internal authors is explained by the SAC in the unity of components such as provision of adequacy of the internal control system, data reliability, and efficient utilisation of the organisation's resources. According to the document's provisions, internal retailers can also prevent and detect fraud and coordinate cooperation with external auditors.

The document entitled Internal Control: Integrated Approach (COSO) (1992) gives recommendations to the management regarding the issues of assessment, description and improvement of the control system. In 2004, COSO published an overall document Managing Organisation Risks: Integrated Approach (COSO ERM). The 12992 documents is an integral part of the 2004 Report, and can be used as a separate document at the same time, The 1992 COSO

report defines internal control as a process, achieved by the organisation's board of directors, management, or some other part of the staff responsible for providing reasonable guarantees of achieving goals in the following categories:

- efficiency and productivity of operations,
- reliability of financial reporting,
- adherence to relevant laws and regulations.

Performing a systemic approach, the report points out that the internal control system represents an instrument rather than a substitute for management, and that control tools must be integrated into the operating activities (rather than built on its basis). Although internal control is defined as a process in the report, it is recommended that the internal control's efficiency assessment should be carried out at a certain moment.

According to the provisions of the COSO document, activities related to carrying out the information system control include norms and procedures, which provide execution of the management's directives by the staff. Activities related to carrying out the control include reconsideration of the control system, physical control tools, task delegating and information system control tools. The information system control tools can be divided into general and applied control tools. The general control tools are the tools that encompass the right of access, software and system development. Applied control tools are the tools preventing mistakes due to system implementation or detect and correct mistakes existing in the system.

The organisation receives information and disseminates this information within the organisation. The information system determines and provides reports on financial and operative information, which are useful for controlling the organisation's activity. Within the organisation, the staff should receive a message that they must understand their roles in the internal control system, to have a serious attitude to their obligations in terms of internal control, and, if necessary, inform the management about problems. Outside the organisation, physical persons and organisations supplying or taking over goods and services should receive a message that the organisation does not allow inappropriate actions.

Further documents - instructions about considering the internal control structure within the financial reporting audit, are methodological instructions for external auditors regarding the influence of internal control on planning and carrying out the audit of an organisation's financial reporting. These two documents primarily emphasise reliability of financial reporting, but they also refer to the issues of control in the area of information systems and communications. So, for instance, SAS 78 replaces 3 elements of internal control structure of SAS 55 (control environment, accounting system, control procedures) with 5 components of the internal control system laid out in the COSO (control environment, risk assessment, activities on control performance, information and communication, monitoring).

Demonstrating in full the systemic methodological approach, each of the analysed documents focuses on internal control and a specific target group (for example, internal auditors, management, information system auditors, external auditors etc.) and pays considerable attention to creating and accessing internal control tools and the issues of risk assessment and management. Regardless of a certain difference between these documents, and some inconsistencies, which are mainly related to the fact that they were prepared by different entities for different target groups from the very beginning, the issue of information technologies system control is elaborated to a greater or lesser extent in each document, which once again confirms the relevance of this problem and defines the methodological base for further study of it.

5. Application of self-assessment as a practical model of identifying IT risk in internal audits

Comparison of content and methodological bases of the five analysed documents used in contemporary practice for assessing risks for the purpose of internal audit, these documents apparently differ in the issues of target group, at which they are aimed, the goal that is to be achieved, and the level of detail elaboration.

Although each of the above presented documents has a methodological significance for assessing risks that were connected with the use and application of information technologies in organisations, its differences are also worth mentioning: COBIT is intended for three target groups: management, users and information system auditors, SAC is mostly designed for internal auditors, COSO is for managers and boards of directors, and SAS 55/78 is predominantly or

external auditors. However, as a whole, these five documents supplement and support each other and are useful from the methodological point of view for essential target groups (management, lawyers, shareholders), but also for other persons interested in understanding and improving internal control and application of the self-assessment procedure, as one of the possible practical models with great potential for identifying risks related to the application of information technologies in internal revision.

The Control Self-Assessment (CDA) in the area of applying information technologies is understood in this paper as an all-embracing and systematic analysis of the organisation's activities and its results compared to the selected criteria, i.e. standards of IT operation.

Essential differences between the self-assessment procedure and internal audit are contained in the fact that internal audit represents a type of 'external' monitoring in relation to the process, whereas self-assessment is 'internal' monitoring, within which the process owners evaluate themselves and their own functions. Self-assessment is related to detailed insights into risks, whereas internal audit is intended more for detecting system errors and overall problems. Therefore, the maximum effect for risk management in the area of application of information technologies is achieved by parallel application of both instruments.

As the results of our research indicate, introducing self-assessment into the sphere of utilising information technology in organisations is an instrument with a great potential for determining key risk factors, which is especially important from the aspect of analysing the IT function activities and its results. Still, the priority aspect in terms of applying the self-assessment procedure in internal review is its orientation to providing objective assertions about the risk management system, which is, at the same time, an indispensable condition for further application of this auditing procedure as a management tool.

One of the key possibilities of applying the self-assessment procedure for the needs of internal audit, in our opinion, is related to additional evaluation of self-assessment, which implies testing the received responses and verification of the level of correctness of results by an internal auditor. Thus, we arrive at a conclusion that the self-assessment procedure is not only a management tool in the area of application of information technologies, but also an important internal audit tool, i.e. audit procedure whose basic aim is to provide objectivity in the assessment of the IT risk management system.

A practical model for the application of the self-assessment in the field of applying information technologies in organisations includes using a four-step algorithm:

Self-assessment procedure preparation, which includes defining the basic elements of IT operations for which self-assessment is necessary, selecting questions for each element of risk, making an instruction for filling questionnaires and determining the circle of co-workers from the company who are to perform the survey. The basic elements of IT operations for self-assessment purposes can include the following areas: system configuration, access to information, and responsibility delegation, database management, incident management, the characteristics of the infrastructure (hardware) and its physical environment, system monitoring procedures, compliance with internal and external operating standards, etc.

Data gathering and preliminary processing. The basic methods of gathering information used in the self-assessment process are usually questionnaires (i.e. surveys) and interviews. This step also includes the preliminary processing of data and preparing a 'diagnostic' table of self-evaluation results, with the focus on the relationship between the key elements of IT operations and the company's maturity level according to each of them.

Review of correctness and determining credibility coefficient of answers received within the self-assessment process. The key part of algorithm for applying the self-assessment process which has a large potential for increasing the objectivity in risk measurement and asserting the role of the self-assessment process in terms of providing auditors' guaranties concerns additional testing of the self-assessment result by an internal auditor. As a result of additional testing, it is possible to introduce special coefficients of credibility (i.e. reliability) of the received answers for the entire population, which we regard as one of the ways to overcome the problem of existence of wrong (incorrect) statements, which may give a wrong picture of condition in the area that is the object of self-assessment.

Final analysis of self-assessment results and compiling a report. At this stage, internal audit in cooperation with the IT service managers prepares a report, which should contain the analysis of the

current state of affairs and proposal for the company's transition to a higher level of maturity. The detected problems serve as a basis for determining deadlines and methods (the action plan) for perfecting the key areas of operation in the field of use and application of information technologies that have been identified as problematic.

The foundation of the self-assessment procedure contains the postulate of the necessity to create a stable risk management system based on several interconnected components: definition and categorisation of the key areas of operation; risk management; tools and approaches to (i.e. methods of) risk assessment; management information: skills, resources, training; and continuous enhancement. In the process of elaborating the methodology for the application of self-assessment procedure, within this research, an additional component was added, related to the evaluation of self-assessment of the IT function by an internal auditor. As practice has shown, it is the absence of this component that entails potential problems that can significantly reduce the effect of application of the self-assessment process, such as: reducing the role of internal audit to a mere consulting function, unreliability and unobjectivity of the obtained self-assessment results, inefficiency of risk management, wrong assessment of the corporate management levels, and reducing the potential for enhancing the organisation's overall operations.

6. Conclusion

The problems of establishing, identifying and classifying the risks related to the application of information technologies are one of the fundamental links in the development strategy of modern companies. In relation to this, the inner and outer pressure of a large number of factors existing nowadays motivates not only auditors and the management, but also all other participants in the IT function in the organisation to continuously develop and improve the quality of the risk concept and internal control methods in this area. The normative documents and developed methods dealing with the problems of IT risk management within companies, which we presented in detail in this paper, should become the basic documents determining the general methodology of developing a system of relations between different segments within the company, while the organisation must select independently the practical methods of risks related to the application of information technologies, in accordance with the profile of its activity and accompanying external and internal factors.

We see the application of self-assessment procedure as one of the possible practical methods, which we believe to have a great potential as regards risk assessment in the area of information technologies. In relation to this, it is obvious that the formation and development of a scientifically based self-assessment method, applied for the purpose of internal audit and internal control within the IT functions, whose theoretical basis is currently in the initial phase of formation, will enable not only diminishing corporate risk, but also increasing companies' investment appeal, which represents a competitive advantage of organisations in all spheres of business.

Nevertheless, it is necessary to reiterate the fact that none of the methods used in practice can be the only possible. The implementation process should always be preceded by a process of preliminary analysis, clear definition of goals, balanced and objective consideration of one's own capabilities and planned costs, calculation of working resources and a realistic estimate of required time. The choice of a certain methodological instrument for risk assessment is in direct correlation with the characteristics of operation of a specific organisation (internal and external factors), which actualises the need for further elaboration of models providing a possibility of obtaining results which are more based on empirical data than on experts' assessments. These aspects determine further directions of investigating the observed problem in prospect, and require and interdisciplinary integration of scientific potential for their resolution.

The results of this research also confirm the fact that integration of audit skills and knowledge in the area of application of information system, and also comprehension of the impact of information technologies on the revision process and risk management are not only necessary, but also compulsory competencies for internal auditors in the existent conditions. Currently, such professionals can competently and completely carry out financial, operative and information system audits, and the synergy of knowledge in the areas of auditing and information technologies provides them with great professional and competitive advantage.

References

Beatie, V., Fearnley, S., Brandt, R. (2002). *Auditor Independence and Audit Risk in the UK: A Reconceptualisation*. Retrieved May 15, 2014 from University of Stirling Web site: http://www.stir.ac.uk/

Bernoulli, D. (1954). Exposition of a New Theory on the Measurement of Risk. *Econometrica, 22* (1), 23-36.

Blinova, I., Petrova, D (PwC, 2010). Внутренний аудитор в 2010 году: делать больше при меньших затратах (по результатам исследования PwC)// *Финансовый Директор*, 7-8, 37-42.

Brown, C. E. & Solomon I. (1990). Auditor configure information processing in control risk assessment. *Auditing: A Journal of Practice and Theory, 9* (3), 17-38.

Code of Ethics IIA (2009). Retrieved May 15, 2014 from: https://na.theiia.org:443/standards-guidance/mandatory-guidance/Pages/Code-of-Ethics.aspx

Colbert, J. L., Bowen, P. L. (1996) Comparison of Internal Controls: COBIT, SAC, COSO and SAS 55/78», *Audit and Control Journal 4*, 26-35.

Knight, F. K (2002). *Risk, Uncertainty and Profit*. Washington D.C.: Beard Books.

Sarbanes-Oxley Act of 2002. *Corporate responsibility. Public Law 107–204—July 30, 2002 (107th Congress). 15 USC 7201 note*. Retrieved May 18, 2014 from the US Securities and Exchange Commission web site: http://sec.gov/about/laws/soa2002.pdf

Sennetti, J.T (1990). Toward a more consistent model for audit risk. *Auditing: A Journal of Practice and Theory*, *9* (2), 103-112.

State of the Internal Audit Profession Study (2013). *Reaching greater heights: Are you prepared for the journey?*. Retrieved May, 18, 2014 from: http://www.pwc.com/ca/en/risk/internal-audit/publications/pwc-state-of-internal-audit-profession-study-2013-03-en.pdf

Stanislav Mitrović
Chief Financial Officer Tarkett Eastern Europe
Moscow, Russia
Email: stanislav.mitrovic@tarkett.com