STRATEGIC MANAGEMENT, Vol. 21 (2016), No. 3, pp. 031-042

UDC 005.3
657.6

Received: April 15, 2016
Accepted: July 20, 2016

Internal Auditing and Risk Management in Corporations

Tamara Stojanović
University of Banja Luka, Faculty of Agriculture, Banja Luka, Serbia
Mirko Andrić
University of Novi Sad, Faculty of Economics in Subotica, Subotica, Serbia

Abstract
Global changes force corporate leaders to observe their organizations through the strategic criteria, i.e. business risks they are encountering. New risks, including the new methods of risk assessments and management, have caused the reconsideration of internal auditing's purpose, scope and activities. Traditionally, internal auditors applied risk assessments by themselves in context of planning their audit engagements. However, modern risk-based internal auditing has changed its focus to the analysis and assessment of managers' role in the risk management process, i.e. to the adequacy of total risk management system. Adding value to the risk management process by internal auditing depends on the maturity of this process and moves from the consulting services aimed at establishing and improving risk management process to the assurance on the risk management status. This way, internal auditors provide support to all significant business activities and help their corporations to fulfil their missions.

Keywords
Internal auditing, risk management framework, maturity of risk management process, elements of auditing the risk management process.

Introduction

Corporations' business environment is full of uncertainties (risks) meaning that they cannot have any guaranties for their survival and success. Consequently, a corporation has to manage its risks and the first step is to define its risk appetite. Such risk management approach, including the adequate risk management strategy, represents the necessary precondition for the achievement of the corporation's goals. It enables a corporation to identify and understand its risk exposure, to create and implement the efficient solutions for preventing losses and/or mitigating the negative impact of risks.

Therefore, it is not unusual that internal auditing, being focused on supporting the whole governance process, has become more relevant recently. As a response to the above mentioned this business function has passed through a severe metamorphosis. In the beginning, it was focused on formal and detailed reviews of appropriateness, correctness and reliability of accounting information, but recently it has become a proactive function delivering two types of services. Through the reasonable *assurance* on the efficiency of processes of good corporate governance, risk management and internal controls, but also the *consulting services* aimed at the improvement of all key business areas, internal auditing has been adding value to the quality of whole governance process and therefore enables a corporation to achieve its goals and reduce its risks exposure. (Tušek, 2009).

1. Shift in internal auditing focus

In order to reach the level where it is now, internal auditing has passed a long path of evolution through constant adaptation to the current needs of management and ways of doing business. It is important to keep in mind that from the first definition of internal auditing that was published by Institute of Internal Auditors in 1978, and for the next two decades it was mainly focused on internal controls. Internal auditing based on traditional approach provided the support to a company through independent and objective assurance that the internal controls function in a way as it is required, through the support in better creation and functioning of control system, discovering the internal irregularities and through the support in maintaining better information of relatively isolated senior management (Ratliff, Beckstead, 1994).

Today, it is especially important for internal auditing to be focused on risks or adding value through providing the information needed to recognize, comprehend and assess potential risks. The main contribution of such internal auditing focused on risks – risk-based approach – is that the information, provided as an input to the decision making process, are more valuable to the management just because of the way they are collected. Although the risk has always been a part of internal auditing process, new trends in auditing have brought it to the center of its focus. In traditional approach, internal auditing was focus of risks for the purpose of assessing their own auditing risks. However, in the risk-based approach the focus has been transferred on the analysis and assessment of the *management's role in the risk management process*.

The main characteristics of the old and new internal auditing paradigm and their differences are presented in Table 1.

Table 1 Shift in internal auditing paradigm

Characteristics	Old paradigm	New paradigm
Internal audit focus	Internal controls	Business risks
Internal audit response	Reactive, acting after the events, discontinued, observers in defining strategic plans	Obligatory, in real time, continual supervision, participation in defining strategic plans
Internal audit assessment	Risk factors	Planning by scenarios
Internal audit testing	Significant controls	Significant risks
Internal audit methods	Emphasis on integral and detailed control testing	Emphasis on the significance of coverage of wide business risks
Internal audit recommendations	Internal controls: Strengthen Cost-benefit relation Efficient/effective	Risk management: Avoid/diversify risk Share/transfer risk Control/accept risk
Internal audit reporting	Related to controls	Related to risk processes
Internal audit role in the company	Independent assessment function	Integration with risk management and corporate governance

Source: Selim & McNamee, 1998

The goal of risk-based auditing is to provide the assurance to the management that (Institute of Internal Auditors UK and Ireland, 2003):

- the risk management processes which management has put in place within the organization (covering all risk management processes at corporate, divisional, business unit, business process level, etc.) are operating as intended,
- these risk management processes are of sound design,
- the responses which management has made to risks which they wish to treat are both adequate and effective in reducing those risks to a level acceptable to the board,
- and a sound framework of controls is in place to sufficiently mitigate those risks which management wishes to treat.

The role of the internal auditing in the risk management process has been defined in the International Professional Practices Framework (IPPF). According to Standard 2100 – Nature of Work (The Institute of Internal Auditors, 2012, p. 11), being a part of Performance Standards, internal auditing is explicitly required to contribute to the improvement of risk management. When assessing the adequacy of risk management systems, firstly internal auditors should determine if the key stakeholders or individuals included in the governance process, including the board of directors and auditing committee, understand the methodology of running the risk management process which is specific for the company. Only if this precondition has been met internal auditors may perform their role in providing opinion on the adequacy of risk management process.

2. Risk management framework

Before starting any auditing engagement the first step is to get to know the business environment, conditions and factors affecting the subject of auditing. Considering the risk management process, each internal auditor has, in the first place, to become familiar and comprehend the risk management framework. This framework encompasses all those variables which directly or indirectly affect the risk management process. The risk management framework is multifaceted and according to Spencer Pickett (2005) includes five levels as described below.

1. LEVEL 1: Factors of external and internal environment

- *External global and market developments* such as changing interest rates, international developmnets, fluctuating movement of capital, etc.
- *Statutes, regulations, codes and guidance* – can be generic (common for all corporations) or industry specific.
- *The mission* – one of most important internal factors affecting the risk management process since it defines the nature of corporation's business and its objectives.
- *The chief executive office (CEO) and board* – except for the general overseeing the governance process, the most important contribution of the board is formulation of risk management strategy which should take into account global market forces and the relevant regulatory framework specific for each individual organization (COSO, 2004).
- *Senior management* – should insure that the staff, systems and budgets they are responsible for enabling the implement--ation of risk management strategy.

2. LEVEL 2: Isolation and understanding risk

- *Active stakeholdes* – those stakeholders who have a direct influence over an organization and in the case of corporations they include: shareholders, investors, lenders, associates, partners, employees and others having an improtant influence on the corporation;
- *Passive stakeholders* – do not have a direct influence over the corporation and its decision makers but they affect the way the corporation is seen by the public (e.g. local communities, the media, environmental groups and people concerned about the behavior of large corporations);
- *Strategic risks* – market changes, compliance risk (risk of failing to comply with varous laws and regulations) or failure in meeting the needs of stakeholders, all meaning that the stated mission may not be achieved;
- *Operational risks* – risks of direct or indirect losses as a result of unadequate or weak internal processes, people and systems or external events (Lam, 2003, p. 210);
- *Risk maps* (financial, business, project and compliance) – are used to follow up the impact of strategic and operational risk on different part of an organizations through the classification of all risks in these four categories.

3. LEVEL 3: Risk appetite and factors affecting risk appetite

Risk appetite defines the level of risk an organization is willing to accept and depend on: *capability* of the corporation to understand and manage its risks, *commitment* to the risk management concept, *choices* made or not made in order to achieve business success, *consistency* in risk management approach, *context* of the way an organization operates and deals with its customers and other stakeholders, *challenges*, *communication*, *clarity* of objectives, accountabilities and risk triggers, *controls*, *key values* and *corporate culture*.

4. LEVEL 4: Elements of risk management process

According to enterprise risk management (ERM) model designed by COSO (2004), borad of directors is responsible for the corporate governance, while senior menagement is responsible for risk management process. This means that the senior management is responsible for: formulating business objectives, risk identification, risk assessment, risk management, establishing key performance indicators and disclosures. After the business objectives are formulated and all risks identified, it is necessary to assess these risks as regards their impact on an organization's ability to achieve its objective. One the other hand, it is also important to assess the likelihood of risks to occur unless managed properly.

Depending on how each risk has been assessed, management will decide on risk management approach. There are many possible responses to different types of risk, but four of them, which are most commonly used, include: *avoidance, reduction, sharing and acceptance* (COSO, 2004, p. 53).

Action plans, resulting from the risk assessment process, are aimed at strenghtening controls and improving the way work is planned and performed. Action plans should consolidate all these measures by including the key performance indicators – specific objectives assigned to individuals and/or teams.

Finally, considering the obligations assumed from corporate accountability, i.e. transparency, it is very important to provide adequate disclosers relating to the risk management process.

5. LEVEL 5: Ensuring the continuity of enterprise risk management

In order to ensure the continuity and sustainability of whole ERM framework it is necessary to provide: internal controls, monitoring, validation, improvement and continual integration (Pickett, 2005).

A good ERM process incorporates a good system of *internal control* and a mechanism to update controls as and when risks change in type, impact or likelihood.

Monitoring is necessary to keep the risk management process always up to date and alive. It must be reviewed to ensure that it still does the jos as intended.

Validation ensures a good way of documentation of both: *risk management policies* formulated by the board or *risk management activities* performed on lower levels of an organization. Proper documentation makes monitoring easier to implement and more effective and efficient.

Considering constant changes in external and internal environment, risk management process has to be alive and always developing, *improving*. Therefore, risk management must be set within an environment ready to learn and evolve. If risks are observed as opportunities to learn a lesson and adopt something new and useful, then the whole risk management process reaches a new dimension.

Finally, probably the most important precondition to ensure continuity, efficiency and effectivness of the risk management process is its *integration* into the actual business systems and work methods. Risk management process should be the responsibility of all employees and an integral part of the way people are doing their work.

It can be noticed that the role of internal auditing is mostly significant in this fifth level of risk management framework. Internal auditing as a function of internal supervision ensures the *monitoring* of the risk management process and *documents* the risk management process by its engagements and by its findings. Also, internal auditing *improves* the risk management process by its recommendations and makes the *integration* of the risk management process easier through number of consulting services which help different levels of organisation to become familiar with the risk management methods and more risk aware.

3. Internal audit's role and risk management maturity

According to the official definition of internal audit, formulated by the Institute of Internal Auditors (the IIA), the role of internal audit is to evaluate and improve risk management process where assurance services of internal audit are focused on the evaluation while consulting services are aimed at the improvement of the risk management process (the Institute of Internal Auditors, 2004). The role of internal audit moves between these two types of services – from providing assurance to the board, auditing committee and senior management about the state of risk management to consulting with management to help them improve this process. Which roles the internal audit will assume in each case depend on the maturity of risk management process and the phase it currently passes through.

The extent of internal audit's consulting in ERM will depend on the other resources, internal and external, available to the board and on the risk maturity of the organization and it is likely to vary over time. Internal audit's expertise in considering risks, in understanding the connections between risks and governance and in facilitation mean that it is well qualified to act as champion and even project manager for ERM, especially in the early stages of its introduction. (The Institute of Internal Auditors, 2004, p. 5)

3.1. Determining risk management maturity

Internal auditors simply have to see how they can add the most value in the context of the need to evaluate and improve risk management process. Thus their role can move in the following range (Institut internih revizora, 2009, p. 138):

- no role
- auditing the risk management process as part of the internal audit plan
- providing active, continuous support and involvement in the risk management process, such as participation on oversight committees, monitoring activities and status reporting
- managing and coordinating the risk management process

There are many ways to assess in which risk management maturity phase is an organization currently. One diagnostic tool has been described by Basil Orsini that contains five levels of progressively mature organizational behavior. The various levels of risk maturity are set with five performance indicators (Orsini, 2002):

1. *Organizational Culture* (risk management is performed at every organizational level and is integrated with the organization's management practices; roles and responsibilities are clear; risk management reflects ethics and values as well as sensitivity to legal and political considerations);
2. *Leadership and Commitment* (senior management is committed to establishing risk management at all levels of the organization; there is a multidisciplinary perspective for assessing and responding to strategic and operating risks; a leadership role of senior management);
3. *Integration with Departmental Management Practices and System* (risk management is integrated into business planning and decision-making at the corporate and operational levels, risk measures results have been monitored over time; integration into quality service initiatives; Online access to management information; organization – idea communication);
4. *Risk Management Capability* (continuous risk management training; departmental management tools and techniques are integrated with risk management techniques; multidisciplinary teams provide advice on risk management issues);
5. *Reporting and Control* (scanning of external opportunities and threats; the control environment is linked to departmental objectives and risk appetites and tolerances; there is an accepted level of documentation; measurement and monitoring are in effect).

3.2. Internal audit's input in early stage of risk management maturity

If the risk management process has not been developed in an organization, it is quite understandable to define the audit input in terms of helping to start the risk management process. Although there may be much flexibility in establishing an early audit role, it is very important to agree upon this role with the board and auditing committee, i.e. to put it in an internal audit's charter. In the stage of establishing the risk management process, internal auditors will not be able to perform all the procedures defined by the guidelines of the IIA (see: The Institute of Internal Auditors, 2004). Therefore, the early role of internal audit can be broken down into four basic elements as follows (see: Pickett, 2005):

1. *Facilitation of risk management process*. It assumes the support in starting the process and generally includes risk education by organizing a number of workshops where employees become familiar with the basic risk management approaches and techniques. In the essence, such support should help people understand that they have control over many aspects of their work and to understand the risks affecting the achievement of their business objectives. Also, it is very important to keep in mind that internal auditor should never be responsible for risk management since that is the management's responsibility.
2. *Coordination and Leadership*. This means that internal auditors should be risk champions by promoting the benefits of risk management process, educating an organization's management and staff in the actions they need to take to implement it and by encouraging and supporting them to take these actions.
3. *Help, Support, Design and Implementation.* In an early stage of risk management process internal audit's role can be proactive in a way of helping management to set up the right structures, policies, communication

channels and specific processes that support good risk management and therefore good business management. Activities which can be assumed by internal audit, without taking the responsibility for the risk management process, include: facilitating identification and evaluation of risks; coaching management in responding to risks; coordinating ERM activities; consolidated reporting on risks; maintaining and developing the ERM framework; championing establishment of the ERM; developing risk management strategy for board approval (The Institute of Internal Auditors, 2004, p.1).

4. *Nonaudit Tasks*. In an early stage, when roles and responsibilities have not been clearly defined yet, the board members may assign some tasks to internal audit and consider that their job has been done. However, the IIA has made clear that this trap should be avoided by issuing suitable guidance on the roles that internal auditors should not undertake such as: setting the risk appetite, imposing risk management processes, providing management assurance on risks, taking decisions on risk responses, implementing risk responses on management's behalf, being accountable for risk management (The Institute of Internal Auditors, 2004, p. 2).

3.3. Maturity Stages of Risk Management Process

According to Spencer Pickett (2005), risk management is developing through four stages until reaches its full maturity. These stages are as follows:

1. *Risk Awareness* – considering the internal audit's scope of work (covering all business activities and all processes), its place is quite suitable for spreading the message of risk management importance to the executives and the throughout the entire organization. Risk awareness is being promoted in order to insure that everybody in organization: identifies proactively key business risks, thinks seriously about the consequences of the risks he/she is responsible for and informs higher and lower levels of organization about those risks worth of their attention (Lam, 2003).
2. *Design* – In this stage, internal auditors can add value in a way that they will investigate best practices of risk management in similar organizations as well as in other types of organizations. According to the IIA guidance, depending on the size and complexity of the organization's business activities, risk management processes can be: formal or informal, quantitative or subjective, embedded in the business units or centralized at a corporate level (Institut internih revizora, 2009, p. 138). Risk management process that an organization will adopt should be created in a way that it suits the culture, management style and business objectives of the organization. Thus, in the case of smaller and not very complex organizations, they can establish informal risk committee which will occasionally consider the organization's risk profile and initiate actions accordingly. Internal auditor's task would be to determine if the adopted methodology is comprehensive enough and suitable for the nature of organization's business activities (Institut internih revizora, 2009, p. 139).
3. *Integration* – In this stage, risk management depends on establishing the right structures and business culture. Integration means that risk management process is being seen as a holistic approach applied systematically in order to provide clear accountabilities and effective decision making. It is about: setting good strategy that has been properly thought through, building and maintaining the set of business values that can be translated into policy and then into performance targets and finally into appropriate action.
4. *Review* – Review, monitoring and managerial certification can be established only when a risk management system is in place. This is the stage when internal auditors can start to reduce the extent of their consulting services and start to assume their core assurance role. Assurance services can also be delivered by external auditors and independent experts, but in the case of internal auditors the IIA guidance suggests there are three areas where these assurances may be provided (The Institute of Internal Auditors, 2004, p. 4):

- Risk management processes – both their design and how well they are working
- Management of those risks classified as key – including the effectiveness of the controls and other responses to them
- Reliable and appropriate assessment of risks and reporting of risk and control status.

3.4. Internal audit's input in mature stages of risk management process

Naturally, as the risk management process evolves the role of internal audit changes and its focus shifts from the consulting services to assurance services. In mature stages of risk management, internal audit can still add value through some kind of consulting services such as process facilitation, training and providing advice, but it is more and more oriented to the formal monitoring and objective assurance.

In a mature risk management environment the focus of internal audit work may be (Institute of Internal Auditors UK and Ireland, 2003):

- Auditing the risk management infrastructure, for example, resources, documentation, methods, reporting
- Auditing the whole system of internal control for the complete organization and for individual departments
- Carrying out individual audit assignments that are predominantly about specific risks
- Where a number of risks are controlled through a common system or process, it may be appropriate to perform a combined audit of that system or process.

The result of such a process is expressing the assurance that risks have been managed in a way that is acceptable for the organization, regarding the previously adopted risk tolerance, or facilitating the introduction of necessary improvements relating to the risk management process. According to Griffiths (2006), risk based internal auditing should result in assurance that:

- The management has identified, assessed and responded to risks above the risk appetite
- The responses, especially the system of internal controls treating the risks, are effective in reducing the inherent risks to below the risk appetite
- Where residual risks are above the risk appetite, action is being taken to reduce them to within the risk appetite, or the board has been informed that they will be tolerated, transferred or terminated
- Risk management processes are being monitored by management to ensure they continue to operate effectively.

4. Developing the internal audit's approach

Performance standard 2100 – Nature of work states that: "The internal audit activity must evaluate and contribute to the improvement of governance, risk management, and control processes using a systematic and disciplined approach." (The Institute of Internal Auditors, 2012, p. 11).

Defined like this, scope of internal audit's work can be perceived from the practical angle by looking how internal auditors really add value to the risk management process. In practice, internal auditors add value to the risk management environment by performing following functions (Beumer, 2004):

- Reviewing risk management processes and internal control systems across the organization
- Identifying business risks and assessing internal controls designed to mitigate those risks in terms of reliability, integrity, compliance, protection, efficiency and effectiveness
- Educating the organization with respect to the development and use of cost-efficient risk management processes and the promotion of best practices through internal auditing's role as a change agent.

This focus on risk permeates all aspects of audit work and is nothing new. Strategic reviews, overall assessments of risk management and detailed assessment of particular aspects of risk management framework are all valid audit tasks. Thus, internal auditors support all the relevant business activities and enable an organization to fulfil its mission.

The shift that internal auditing has made over the years has been astonishing. The way it has developed to respond to the growing interest in risk management can be seen in stages that internal audit has been going through (Sobel, 2004):

1. control-based auditing
2. process-based auditing

3. risk-based auditing
4. risk management-based auditing.

In contrast to the risk-based auditing, this new approach – internal auditing based on risk management – expands its focus on key business objectives, management's risk appetite, key performance indicators and risk management capabilities. Instead of being primarily focused on mitigating risks to an acceptable level, in this new approach, internal auditing also considers optimizing key risks where necessary to achieve business objectives. This way, risk management-based auditing becomes a key link of successful risk management process.

The approach of risk management-based internal auditing generally includes following steps:

1. creating an appropriate audit charter
2. creating a risk-based audit plans
3. developing preliminary surveys in audit areas that have been prioritized by risk-based audit plans
4. reviewing the risk registers in use (if any) in the areas under review
5. reporting on risk management and control processes

4.1. Audit charter

Audit charter is the document that defines the position of internal auditing within the context of the risk management policy (approved by the board of directors) and the needs of the audit committee. Internal audit must fit into what is best for specific organization and an audit charter is exactly the document defines its roles and responsibilities. Preparation and application of the internal audit charter should integrate two key factors:

1. board's approach (policy) relating to the risk management, and
2. audit committee's expectations with regards to the internal auditing activities.

Considering these two factors, internal audit charter should enable internal auditors to provide a full range of important services such as following (Pickett, 2005):

- advising the audit committee on the way it is discharging its areas of responsibility
- assisting the board in setting up its published disclosures infrastructure
- encouraging dialogue with key stakeholders so that, wherever possible, their concerns are built into the risk management process
- helping management establish a reliable risk management process and effective internal controls
- promoting compliance with legal and regulatory requirements
- providing assurance and consultancy services that fit in with the other tasks.

Which of the above mentioned activities will be included in an audit charter depend on the specifics of each organization but also on the maturity of its risk management process.

4.2. Risk-based audit plans

The starting place for risk-based audit plans is the 'audit universe', i.e. the list of all those aspects of the organization that can be translated into auditable areas and form the basis of individual audit assignments. Since the audit universe interrelates with the organization's strategic plan (which has been created considering the environment in which the organization operates), it will certainly consider and reflect the overall business objectives but also will be influenced by the results of the risk management process.

When creating their audit plans, internal auditors may and should use all the outputs of the risk management process within the organization, so long as this process is in place and is reliable. One of powerful additional tools that can be used by internal auditors in this case is the corporate risk register. However, risk assessment processes of the internal audit planning process are not sufficient to constitute a proper organizational risk management process (see: Joint Technical Committee, 2004).

It is not excluded that the risk-based audit plans include a wider vision of the organization than might appear at first sight. For example, the auditor may argue that the risk that management, associates, partners and employees may be involved in fraud and abuse should also be included on any corporate risk register. Many feel that ethics is so important that it should be included in the planned audit coverage (Pickett, 2005).

In organization where risk management is not developed at all, it is difficult to use the corporate risk register or other outputs of the risk management process to create the risk-based audit plans. In this case, internal auditing will focus on establishing the process and its running, but will also have to develop a planning mode that can be used to support the annual audit plan. There is a variety of risk models assisting the chief audit executive in prioritizing potential audit subject areas. Most risk models utilize risk factors such as: financial impact; asset liquidity, management competence, quality of internal controls, degree of change or stability, time of last audit engagement, complexity, employees and government relations, etc. (Institut internih revizora, 2009, p. 124).

Finally, one should keep in mind that the risk-based audit plans have always to be updated in order to be aligned with the direction of the organization.

4.3. Preliminary survey

Preliminary audit survey represents an attempt to perform some background work so that audits from the risk-based annual plan can be properly structured and planned, i.e. so that long-term plans can be translated into the assignment plans. Besides the ERM framework that significantly determine the way of performing the preliminary survey, there are two additional tools facilitating these surveys – *control and risk self assessment (CRSA) and questionnaires*.

ERM framework provides initial information that internal auditors need to perform preliminary survey, but, at the same time, these auditing activities will help auditors to determine if the ERM really fulfils its purpose or not.

Internal auditors may also use *CRSA* to facilitate and progress the audit process. *CRSA* has become really popular and accepted practice recently and it has been used in private/profit but also in public and non-profit sector. The reason why it has become so popular is that it refers to people that live in real world and deal with real problems by using their own knowledge and capabilities. But maybe the reason is also that finally it has become clear that the main cause of organizations' success is people and not the procedures (Sawyer, Dittenhofer, & Scheiner, 2003).

Internal auditors can use the *CRSA* in two ways. The first is to rely on any CRSA events that have recently been employed but the staff from the area that is being reviewed. If this process is sound and well documented, the auditors may be able to use the outputs to drive the terms of reference for the proceeding audit. In the other case, it is the internal auditor who organizes the CRSA workshop by getting key people from the area under review together and then he uses the outputs form this audit-driven CRSA workshop to develop and finalize the terms of reference for the audit.

The second tool internal auditors may use in their preliminary survey relates to *questionnaires* that can be sent out to people in the area under review before the audit is started. The idea is to gather relevant information about the control status and the level of control awareness and to use these findings to help focus the planned audit. Questionnaires, followed up with a few interviews, can be used to assess the state of control awareness, and based on this assessment internal auditors can also plot trends over a period to see if this awareness is improving or not. Based on questionnaires results, the audit work can then be focused on those areas where control cultures are poor.

4.4. Assignment plan and business risk register

According to performance standard 2200, internal auditors must develop and document a plan for each engagement, including the engagement's objectives, scope, timing, and resource allocations (The Institute of Internal Auditors, 2012). This plan sets out exactly what will be done and who will do what. In the *assignment plan*, internal auditors must determine appropriate and sufficient resources to achieve engagement objectives based on an evaluation of the nature and complexity of each engagement, time constraints, and available resources (Performance Standard 2230, The Institute of Internal Auditors, 2012).

When considering assignment plans for evaluating risk management process *business risk register* has a crucial role. Business risk register can be created through the reviews by the manager and management team, or the risk workshops where the teams reporting up to the manager discusses the risks, or through an assessment of intelligence and trend analysis. It is basically a data schedule that helps understand the whole risk profile of an organizations by including some key elements such as: risk description, type of risk (financial, operational, project...), risk impact (its consequences), risk likelihood, level of risk (the result of multiplication of previous two items), description of controls (if any) established to mitigate the risk, actions planned as a response to the risk, identification of stuff responsible for the risk management.

Before making a final opinion on total effectiveness of risk management and control processes, internal auditors should provide answers to three more questions (Institut internih revizora, 2009, p. 143):

- Were significant discrepancies or weaknesses discovered and other assessment information gathered?
- If so, were corrections or improvements made after these discoveries?
- Do the discoveries and their consequences lead to the conclusion that there is a pervasive condition resulting in an unacceptable level of business risk?

To answer these questions internal auditors should provide (gather and create) extensive documentation in form of *audit evidences*. The essence of this evidence is to help an auditor to reach the confirmation whether current business activities, i.e. the elements of the adopted ERM framework, are effective of not.

If there is no business risk register in the organization, internal auditors' task is to provide consulting to the management in this respect. In the meantime, they have to make total assessment of risks and controls for the area under the review by themselves.

4.5. Reporting on risk management and control processes

Communicating the status of risk management process includes the assessment, i.e. opinion on efficiency and effectiveness of internal controls in business segment under the review. Communications must include the engagement's objectives and scope as well as applicable conclusions, recommendations, and action plans (Performance Standard 2410, The Institute of Internal Auditors, 2012). Also, the audit reports have to meet certain quality standards meaning that they must be accurate, objective, clear, concise, constructive, complete, and timely (Performance Standard 2420, The Institute of Internal Auditors, 2012).

Although the format and contents of final audit engagement report might differ depending on the organization or type of engagement, it should always contain at least three elements:

1. *Purpose of engagement* – describing the engagement objectives and informing the readers on the reasons why the audit engagement is being performed and what is expected from it
2. *Scope of engagement* – specifying audit activities and, if appropriate, providing the information on time period covered by the engagement
3. *Engagement results* – including the audit findings, conclusions, opinions, recommendations and action plans.

According to the IIA Practice Advisory 2410-1 (Institut internih revizora, 2009), e*ngagement observations and recommendations* emerge by a process of comparing what should be with what is. Whether or not there is difference, the internal auditor has a foundation on which to build the report. When conditions meet the criteria, acknowledgment in the engagement communication of satisfactory performance may be appropriate. Observations and recommendations should be based on the following attributes (Institut internih revizora, 2009, p. 174):

- **Criteria**: The standards, measures or expectations used in making an evaluation and/or verification (what should exist)
- **Condition**: The factual evidence that the internal auditor found in the course of the examination (what does exist)
- **Cause**: The reason for the difference between the expected and actual conditions (why the difference exists)
- **Effect**: The risk or exposure the organization and/or others encounter because the condition is not consistent with the criteria (the impact of the difference).

Conclusions and opinions are the internal auditor's assessments on the effects that auditing observations and recommendations have on the area subject to audit. *Conclusions* may include the whole range of engagement aspects or some specific aspects of engagement. They can include even the conclusions on whether the business or program objectives are in line with the organization's objectives, if the organization's objectives have been achieved and if the business activities under the reviews function as it was planned or not. *The opinion* may include the overall assessment of controls or just the assessment of controls in the area under the review, or it can be limited to some specific controls or aspects of engagement.

Internal auditor's report can also include the *recommendations* for improvements, *praises* for good performance and *correction measures*. During the discussions with the 'engagement client', internal auditor should try to reach the agreement on the engagement results and any action plan that is needed to improve the business operations. If there is a disagreement between internal auditor and the engagement client, the report should contain both standpoints and the reasons for disagreement.

After the engagement is finished, chief audit executive submits a signed report. Report summaries, specifying only the engagement results, are suitable for senior management (above the engagement client) and can be submitted separately or together with the final report.

The internal auditing report is the final products of the whole auditing process and should be a confirmation of the internal audit's contribution to the whole risk management process and a proof that internal auditing has done its job in order to add value to the organization.

Conclusion

Corporate governance represents the mix of numerous aspects which goal is to meet the characteristics and achieve the objectives of corporate governance. The first and basic goal is to fulfil the expectations of all stakeholders and that is very often difficult to realize because of their conflicts of interests. Therefore, internal auditors should not only be familiar with all the characteristics and aspects of corporate governance, but they are also expected to evaluate the systems that have been established to achieve the goal of corporate governance. Therefore, internal auditors add value to the business by providing the assurance to the stakeholders that the systems, established to insure their expectation and interests, are efficient and effective.

When considering the way internal auditing adds value to the risk management process in corporations, we can conclude that its role varies among organizations and depending on the maturity of risk management process. Therefore, the first task of internal auditing is to determine the level of risk management maturity and to forecast the trend of the risk management development. Then, internal auditing starts to deliver its services on the current level of risk management maturity by providing adequate support in establishing the structures and risk management approaches (consulting services in early stages). As an organization becomes more and more mature and capable to manage its risks, internal auditing focuses more on providing objective assurance in contrast to the earlier role of business consultant, educator and facilitator.

Internal audit's approach based on the risk management process enables it to be a pioneer of these processes by assessing risks in all areas and providing the timely signals to the board and management in order to add value to the organization and help achieving its goals and objectives. SM

References

Beumer, H. (2009). *Starting from Scratch. Internal Auditor.* Retrieved October 2009 , from http://findarticles.com/p/articles/mi_m4153/is_4_61/ai_n6169119/

COSO. (2004). *Enterprise Risk Management – Integrated Framework, Executive Summary.* Retrieved February 26, 2016 , from http://www.coso.org/documents/coso_erm_executivesummary.pdf

Griffiths, D. (2006). *Risk Based Internal Auditing: Three Ways of Implementation.* Retrieved May 2014, from Risk Based Internal Auditing: http://www.internalaudit.biz/files/implementation/Implementing%20RBIA%20v1.1.pdf

Institut internih revizora. (2009). *Međunarodni okvir profesionalne prakse (IPPF).* Sarajevo: Udruženje internih revizora u BiH.

Institute of Internal Auditors UK and Ireland. (2003). *Position Statement on the Risk Based Internal Auditing.* Retrieved December 2009, from Chartered Institute of Internal Auditors: http://www.iia.org.uk/en/other/document_summary.cfm/docid/B70D0EC9-4BDC-4058-B48CABFDEC2F37C5

Joint Technical Committee. (2004). *Australian/New Zealand Standard, Risk Management Guidelines.* Sydney: Standards Ausralia International.

Lam, J. (2003). *Enterprise Risk Management.* New Jersey: John Wiley & Sons.

Orsini, B. (2002). *Mature risk management: a benchmarking tool from Human Resources Development Canada facilitates assessments of risk management practices in the organization - Risk Watch.* Retrieved December 2009, from Find Articles: http://findarticles.com/p/articles/mi_m4153/is_4_59/ai_90257866/?tag=content;col1

Pickett, S. K. (2005). *Auditing the Risk Management Process.* New Jersey: John Wiley & Sons.

Ratliff, R. L., & Beckstead, S. M. (1994). *How world-class management is changing internal auditing. Internal Auditor.* Retrieved December 2009, from Find articles: http://findarticles.com/p/articles/mi_m4153/is_n6_v51/ai_16529834/

Sawyer, L. B., Dittenhofer, M. A., & Scheiner, J. H. (2003). *Sawyer's Internal Auditing.* Orlando: Institute of Internal Auditors.

Selim, G. M., & McNamee, D. (1998). *Risk Management: Changing the Internal Auditor's Paradigm.* Florida: The Institute of Internal Auditors Research Foundation.

Sobel, P. J. (2004). *Integrating Risk Management and ERM. Auditors Risk Management Guide.* Chicago: CCH Incorporated.

The Institute of Internal Auditors. (2012). *International Standards for the Professional Practice of Internal Auditing (Standards).* Retrieved January 5, 2016, from The Institute of Internal Auditors: https://na.theiia.org/standards-guidance/Pages/Standards-and-Guidance-IPPF.aspx

The Institute of Internal Auditors. (2004). *The Role of Internal Audit in Enterprise-Wide Risk Management, Position Statement.* Retrieved February 26, 2016, from

The Institute of Internal Auditors: https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Role%20of%20Internal%20Auditing%20in%20Enterprise%20Risk%20Management.pdf

Tušek, B. (2009). Povezanost interne revizije i procesa upravljanja rizicima poduzeća u Republici Hrvatskoj – empirijsko istraživanje. *HZRIFD, 12. savetovanje na temu interna revizija i kontrola.*

✉ **Correspondence**

Tamara Stojanović

Faculty of Agriculture
Bulevar vojvode Petra Bojovića 1A, 78 000 Banja Luka, Bosnia and Herzegovina

E-mail: tamara.stojanovic@agrofabl.org