Improvement of Business and IT Alignment through IT Internal Audit

Silvana Tomić Rotim
ZIH – Zavod za informatičku djelatnost Hrvatske d.o.o.
Mažuranićev trg 8, 10000 Zagreb
e-mail: stomic@zih.hr

Višnja Komnenić
HEP d.d.
Ulica grada Vukovara 37, 10000 Zagreb
e-mail: visnja.komnenić@hep.hr

Abstract.
This paper shows the overview of models used for business and IT alignment (COSO, CobIT, IT Balanced Scorecard etc.) and their interrelationships. We present the results of international audits according to control areas by CobIT and the most important findings, especially identified weaknesses. The general result of these audits is awareness and willingness of top management to align business and IT, but with minimal compliance costs. We describe the process of IT internal audit and performance monitoring at business and IT levels, based on risk assessment through testing implemented controls. It shows the relationships between business and IT objectives and metrics, and it could be used for detecting broken connections between them. It is a great opportunity for recognition of improvement areas for aligning business and IT. Because of that, the final result of IT internal audit is not a report by an internal auditor but monitoring the realization and implementation of agreed improvements. It should lead continuously to better aligned business and IT.

Keywords. Business and IT Alignment, COSO, CobIT, IT Balanced Scorecard, IT Internal Audit

1. Introduction

Information technology has been recognized for its potential to contribute to sustained advantage for companies, however, research on the relationship between information technology spending and firm performance has produced inconsistent results, leading many to note an apparent "Productivity paradox". This potential hazard is possible to reduce using different models for business and IT alignment that could result in improving company performance. For that purpose, it is useful to apply some of different alignment models, such as COSO, CobIT, IT Balanced Scorecard and others, as well as, their combination. In this paper we have described how these models could be closely related and implemented through internal audit as a tool that could help in solving above mentioned paradox.

Here it has been observed IT Internal Audit as a part of whole Internal Audit, and its role in collecting and assessing evidence on whether IT operates in accordance with company asset protection, data integrity maintenance, efficient support of company's goals and efficient use of information resources with the main objective of achieving high level of business and IT alignment. It has been presented for one Croatian company.
The main objective of IT internal audit is to examine and check whether the information system is set within defined criteria of available business processes and resources functioning and aligned to business system, bearing in mind basic IT functioning criteria which are: efficiency, effectiveness, confidentiality, integrity, availability, compatibility and reliability. IT

internal auditors therefore analyze information systems and their operations through risk assessment, evaluation of internal control and internal control system in order to ensure the existence of prescribed risk mitigation control within company's information system to a minimum i.e. to an acceptable level. Risks can be defined as "a probability of negative events or activities appearance, which can affect a non accomplishment of set company goals as a whole".

As a source for evidences of IT performance in a function of business performance achieving, IT BSC performance management system could be used. IT internal audit and its result is a good base for continuous improvement, further alignment of business and IT and achievement of business performance.

2. Business-IT Alignment Models

Businesses have invested enormous sums in information technology, and the challenge they have faced is how to optimize these investments. Many studies have been investigated the moderating affect of business-IT alignment on the relationship between IT investment and company performance [1, 2]. The alignment of IT strategy with business strategy has been touted as a critical element of IT management.

There are many frameworks that could be used for solving this critical element, starting with COSO used by the finance group to build their business processes and associated controls, and after that CobIT that takes many of the objectives of COSO and translates them into a framework that IT people used for aligning IT processes with business processes. That could be resulted in better business performance. For monitoring and assessing business and IT alignment through achieved performance it could be used Balanced Scorecard in business domain, and IT Balanced Scorecard in IT domain. The short explanation of the mentioned frameworks is listed hereafter.

2.1. COSO Framework

The COSO framework (Committee of Sponsoring Organizations of the Treadway Commission) was updated in 2004 as COSO2 to reflect the changed reality of the world. To break it down further, COSO consists of eight different components:

- Internal control environment
- Objective setting
- Event identification
- Risk assessment
- Risk response
- Control activities
- Information and communication
- Monitoring

This model offers a linkage between three principles of Enterprise Governance: Corporate Governance, Internal Control and Risk Management. The above mentioned components are the components of Enterprise Governance, and they are directly connected with objectives that an organization strives to achieve. The relationship is depicted in the three-dimensional matrix, figure 1.

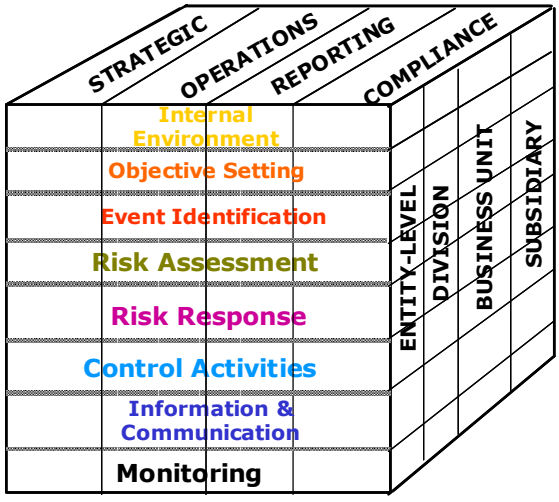

Figure 1 COSO cube, [5]

The internal environment encompasses the tone of an organization, influencing the risk consciousness of its people, and is the basis for all other components of enterprise governance, providing discipline and structure. Internal environment factors include an company's risk management philosophy, its risk appetite, oversight by the board of directors, the integrity, ethical values, and the competence of the company's staff, and the way the management assigns authority and responsibility, and organizes and develops its people.

Objectives are set at the strategic level, establishing a basis for operations, reporting, and compliance objectives. Every company faces a variety of risks from external and internal sources, and a precondition to effective event

identification, risk assessment and risk response is establishment of objectives. Objectives are aligned with the company's risk appetite which drives risk tolerance levels for the entity.

Management identifies potential events that, if they occur, will affect the company and determines whether they represents opportunities or whether they might adversely affect the company's ability to successfully implement strategy and achieve objectives. Events with negative impact represent risks, which require management's assessment and response. Events with positive impact represent opportunities, which management channels back into strategy and objective-setting processes. When identifying events, management considers a variety of internal and external factors that may give rise to risks and opportunities, in the context of the full scope of the organization.

Risk assessment allows an entity to consider the extent to which potential events have an impact on achievement of objectives. Management assesses events from two perspectives – likelihood and impact – and normally uses a combination of qualitative and quantitative methods. The positive and negative impacts of potential events should be examined, individually or by category, across the company. Risks are assessed on both an inherent and residual basis.

Having assessed relevant risks, management determines how it will respond. Responses include risk avoidance, reduction, sharing and acceptance. In considering its response, management assesses the effect on risk likelihood and impact, as well as costs and benefits, selecting a response that brings residual risks within desired risk tolerances. Management identifies any opportunities that might be available, and takes an company-wide, or portfolio, view of risk, determining whether overall residual risk is within the company's risk appetite.

Control activities are the policies and procedures that help to ensure that management's risk responses are carried out. Control activities occur throughout an organization, at all levels and in all functions. They include a range of activities – as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties.

Pertinent information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Information systems use internally generated data and information from external sources, providing information for managing risks and making informed decisions relative to objectives. Effective communication also occurs, flowing down, across, and up the organization. All personnel receive a clear message from top management that enterprise governance responsibilities must be taken seriously. They understand their own role in enterprise governance, as well as, how individual activities relate to the work of others. They must have a means of communicating significant information upstream. There is also effective communication with external parties such as customers, suppliers, regulators and shareholders.

Enterprise governance is monitored – assessing the presence and functioning of its components over time. This is accomplished through ongoing monitoring activities, separate evaluations or a combination of the two. Ongoing monitoring occurs in the normal course of management activities. The scope and frequency of separate evaluations will depend primarily on an assessment of risks and the effectiveness of ongoing monitoring procedures. Enterprise governance deficiencies are reported upstream with the serious matters reported to top management and the board.

2.2. CobIT Framework

CobIT (Control Objectives for Information and related Technology) is a comprehensive set of resources that contains all the information organizations need to adopt IT governance and control framework, and its starting point is business strategy as a base for generating business goals for IT then IT goals [3]. CobIT contributes to company needs by:

- Making a measurable link between the business requirements and IT goals
- Organising IT activities into a generally accepted process model
- Identifying the major IT resources to be leveraged
- Defining the management control objectives to be considered
- Providing tools for management: goals and metrics to enable IT performance to be measured, maturity models to enable process capability to be benchmarked, responsible, accountable, consulted and

informed charts to clarify roles and responsibilities.

It is well-presented through CobIT cube that is shown in figure 2.

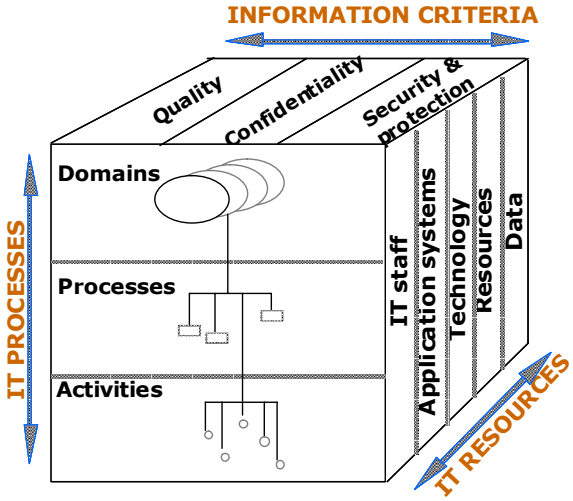

Figure 2 CobIT cube

CobIT is a methodology outspread through the whole world. There are some experiences in using CobIT in Croatia too [8]. CobIT has been used for improving current situation of using IT and through its better using, achieving higher business efficiency and effectiveness.

Comparing these two models it is possible to notice that COSO addresses application controls and general IT controls at a high level and doesn't dictate requirements for control objectives and related controls activity. At the same time CobIT is a comprehensive framework for managing risk and control of information technology and it has 318 detailed control objectives. CobIT is COSO compliant [6].

2.3. IT Balanced Scorecard

The measurement of effectiveness of COSO components through achievement of organization's objectives and CobIT objectives in IT domain could be realized through Balanced Scorecard and IT Balanced Scorecard. Their fundamental premise is that the evaluation of a firm should not be restricted to a traditional financial evaluation but should be supplemented with measures concerning customer / user satisfaction, internal business and IT processes and the ability to innovate. In Figure 3, a generic IT Balanced Scorecard is shown [7].

BUSINESS CONTRIBUTION
Perspective question How does management view the IT department? ***Mission*** To obtain a reasonable business contribution from IT. ***Objectives*** • Control of IT expenses • Business value of IT projects • Provision of new business capabilities
USER ORIENTATION
Perspective question How do users view the IT department? ***Mission*** To be the preferred supplier of information systems. ***Objectives*** • Preferred supplier of applications • Preferred supplier of operations • Partnership with users • User satisfaction
OPERATIONAL EXCELLENCE
Perspective question How effective and efficient are the IT processes? ***Mission*** To deliver effective and efficient IT systems and services. ***Objectives*** • Efficient and effective development efforts • Efficient and effective operations
FUTURE ORIENTATION
Perspective question How well is IT positioned to meet future needs? ***Mission*** To develop opportunities to answer future challenges. ***Objectives*** • Training and education of IT staff • Expertise of IT staff • Research into emerging technologies • Age of application portfolio

Figure 3 Generic IT Balanced Scorecard

The User Orientation perspective represents the user evaluation of IT and the level of realization of CobIT objectives visible through user perspective. The Operational Excellence perspective represents the IT processes employed to develop and support the applications – CobIT

processes. The Future Orientation perspective represents the human and technology resources needed by IT to deliver its services over time. The Business Contribution perspective captures the business value created from the IT investments and directly is connected with business objectives set at all levels through COSO component – Objective Setting.

Each of these perspectives has to be translated into corresponding metrics and measures that assess the current situation. These assessments need to be repeated periodically and aligned with pre-established objectives through COSO components and CobIT in IT domain – Plan & Organize. The relationship between these three models is represented through a matrix in Figure 4. IT BSC links with business BSC through financial – contribution perspective and together become a linked set of measures for aligning Enterprise Governance (COSO) with IT Governance (CobIT) and determining how business value is created through information technology. Through Internal Audits it is possible to monitor this set of measures and the results of them use for continuous improvement in business – IT alignment.

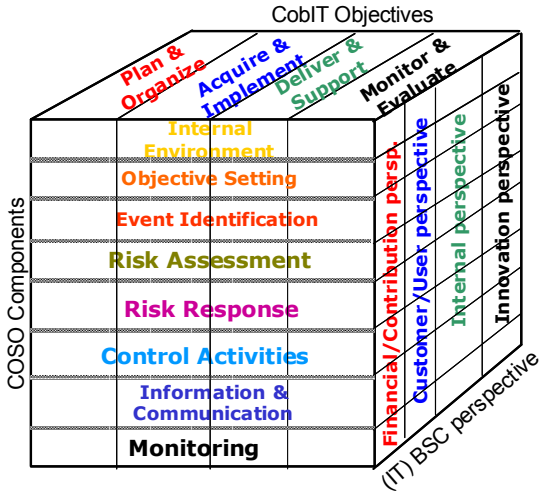

Figure 4 COSO – CobIT – (IT) BSC matrix

3. Results of international audits

It was done more independent information system audits in banks and financially consolidated subsidiaries based on CobIT framework [4]. Before the IS audit, management assumed CobIT audits as one more useless regulation, waste of time, new cost and it didn't recognize need to understand IT issues.
After the IS audit, the situation has been changed. Management has realized that finding would be very helpful for them to create the control environment in IT, and necessity for aligning business and IT. They have been interested in understanding IT Governance and monitoring every dollar spent in IT.
The strengths identified in IT processes were:

- Physical Environment Management
- Application Software Acquisition and Maintenance

The weaknesses identified in IT processes were:

- IT Strategy
- Business IT Alignment
- IT Risk Management
- Business Continuity Management
- IT Service Management
- IT Project Management
- IT Internal Control

The main question was how to solve the weaknesses and comply to the most suitable model, but with minimal costs. As a solution it is recognized Integrated Assessment Programs based on risk approach. The way of implementing that in internal audits in a real company is described in the next paragraph.

4. Process of IT Internal Audit

IT internal audit is a process of collecting and assessing data, followed by establishing evidence and defining findings on the quality of company IT system. The main task of information system internal audit and the use of IT support is to obtain reliable and accurate data in according IT security, asset protection, data integrity maintenance and to improve efficiency and effectiveness of whole company's operations, with the aim of accomplishing company policy goals [13].

One of the reasons why information system internal audit in companies is necessary is the fact that protection of IT system integrity has become an important business issue in today's conditions, when companies' core activities are becoming more tightly linked with their information

systems. The computer auditing (IT auditing) is a sine qua non of the modern companies [9].

There are three main reasons for performing an information system audit [14]:

1. Availability – check whether the IT system and all relevant data on business processes will be available to appropriate persons at all times. Is company's IT system adequately protected from all types of losses and disasters?
2. Confidentiality – check whether access to data in the IT system will be granted only to persons who need to see and use them, i.e. will they be protected against deliberate and unintentional disclosure to unauthorized persons?
3. Integrity – check whether data, which are a product of the IT system, will always be accurate, reliable and timely. In what way are unauthorized changes in the data or software within the IT system prevented?

The main objective of IT internal audit is to examine and check whether the information system is set within defined criteria of available business processes and resources, bearing in mind basic IT functioning criteria which are: efficiency, effectiveness, confidentiality, integrity, availability, compliance and reliability. IT internal auditors therefore analyze information systems and their operations through risk assessment process, evaluation of internal control and system of internal controls in order to ensure the existence of adequate controls within company's information system for risk mitigation to a minimum i.e. to an acceptable level.

Just like all IT systems, HEP d.d. IT system has its weaknesses, which may pose different kinds of risks for the company. Weaknesses may occur in hardware architecture, operation systems configuration, software design and its use or within processes. In accordance with that, since the introduction of internal auditing in HEP d.d., several types of audits have been performed based on risk assessment.

4.1. Risk Assessment, Threat and Information System Vulnerability Analysis

Regardless whether it concerns IT security or other types of risk, risk assessment is a means of providing information to all those involved in decision making, so they could understand factors which may have a negative impact on business activities and results, as well as form a good judgment regarding the scope of necessary risk mitigation activities.

Risk assessment was a necessary needed as a means to help carry out audit responsibility to identify areas in which audit work will add value to the organization, as well as to support governance and control processes in the company.

So, the main questions internal auditors asked were as follows:

1. How efficient is internal audit in the organization? In other words, the question is: assuming the process of audit is efficient, how can the internal audit function make a maximum contribution to the organization through the internal audit work?
2. To what extent does internal audit fulfill its duty to cover critical processes in the organization? In other words, how much can we rely on internal audit function in obtaining a complete and precise picture on organization's activities? This is a key question when we consider cases such as Enron, WorldCom etc., where there were issues regarding internal auditing efficiency within the control and governance processes.
3. What are the necessary resources to fulfill the internal audit duty? Can we anticipate the scope of required know-how and work force necessary for meeting our responsibilities?

Those and other topics were main issues that lead to the implementation of risk management methodology in auditing. Up-to-date professional standards were also established, which now require the use of risk assessment technique in the process of preparing an internal audit plan in general, as well as performing certain auditing tasks.

In the process of IT internal audit it is also necessary to identify, evaluate and analyze possible risks regarding information systems. When performing an IT internal audit it is

necessary to identify and assess possible risks in order to focus the audit on precisely those risks whose occurrence would have the biggest impact on IS system, and to make the audit sense. Risk assessment includes identification and analysis (valorization and ranking) of relevant risks which have an impact on company's goals, so it could be established how to manage those risks successfully and how to reduce them to an acceptable level.

Today's companies have a complex business structure. This complexity is a result of globalization and the opening of world markets, as well as technological changes and the entry into an era of e-business, government regulations, international global trade agreements and ecology. The business complexity faces (exposes) the organization with new risks. In fact, today's managers are required to manage risks on daily basis in order to fulfill company's business plan.

In risk management theory there are two different types of risk:

1. Inherent risk – which refers to the potential occurrence of an undesired event due to a lack of specific control and
2. Residual risk – which refers to the potential occurrence of an undesired event despite existing mitigation controls built to minimize the risk.

This section demonstrates that we are dealing with a relative risk analysis. However, it is almost impossible to minimize risk to the absolute zero level.

In order to deal with risk successfully, it needs to be marked (mapped) with two parameters:

- Likelihood of risk occurrence and
- Impact (materiality), i.e. the impact of risk and the biggest possible damage an exposure or undesired event could cause.

Mapping risk is not an easy task, since two parameters necessary to calculate risk level cannot be quantified or accurately calculated. It needs to be stated that different people would evaluate the likelihood of the same event differently and quantify the damage which might occur as a result of such event in a different way. We are therefore dealing with an equation that consists of two unknown parameters.

Risk can be defined as a likelihood of negative events which can have a negative impact on the accomplishment of set company goals.

In order to identify potential risk in the information systems and its security, we use several questions, such as: What is the source of threat to company's IT system?, What kind of damage will be done to company's activities if a certain threat is carried out?, What are the reasons for concern?, What are the existing controls with regards to such threats?, What are the existing protection (security) and control measures, if any? and What protection (security) and control measures should be implemented in order to protect our IT system adequately?
The next step is to identify possible threats to our IT.

After identifying potential threats, we need to identify IT assets and services which are most liable to those threats. While doing so, special attention needs to be paid to: IT environment (rooms where IT equipment is kept – offices, data centers and rooms where electrical, network and other equipment is kept), employees – who work with IT equipment, data – all data kept on servers or local PC's, software – all existing and development software, hardware – all IT equipment (servers, PC's, network equipment etc.) and IT services – e-mail, the Internet, the Intranet etc.

After completing those steps, we can move on to assessing potential risks in IT systems, using basic criteria for risk assessment: likelihood of risk occurrence and the impact (materiality) it can have on company's activities (Figure 5, Figure 6 and Table 1). By ranking risks using the risk assessment matrix we can obtain a list of most significant risks, which will be the object of auditing process, that is, a list of internal audits with risk assessment (Audit Universe) will be made accordingly.

Table 1. Risk assessment table

No.	Type of risk	Likelihood	Impact (Materiality)	Total (3x4)
1	2	3	4	5
1	Risk			
2	Risk			
3	Risk			

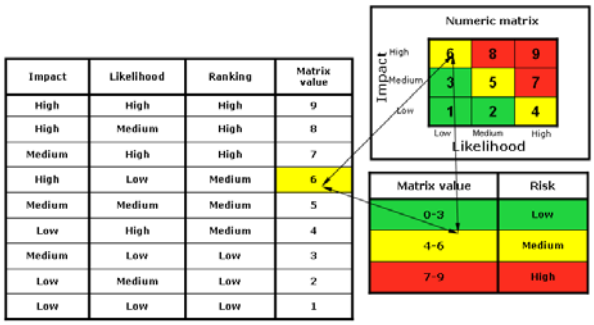

Figure 5. Risk assessment matrix

According to risk assessment at the end of each year, internal auditing department in HEP d.d. makes a list of internal audits with risk assessment (Audit Universe) to be performed, in order to plan their work more efficiently and draw up an annual auditing plan. The risk based approach is therefore the approach used in performing internal audits in HEP d.d., since identifying risk requires know-how, experience and good knowledge of business process.

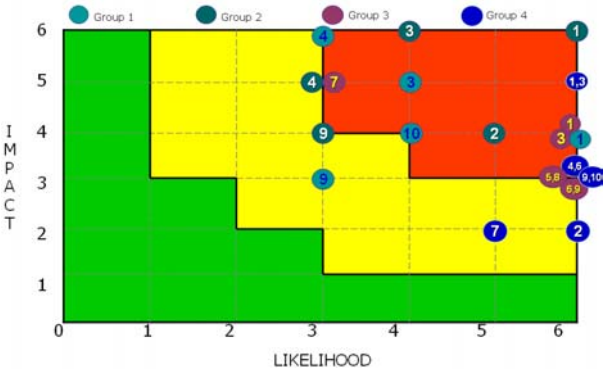

Figure 6. Risk assessment matrix in IT (in HEP d.d.)

4.2. The Stages of IT Internal Audit

The process of IT internal audit in HEP d.d. is a process of applying appropriate standards and publications (e.g. ISO 17799 and ISO 27001, COBIT, etc.), internal audit standards (IIA Standards, ISACA Standards, HIIR Standards), HEP d.d. internal acts, as well as standards and criteria for assessing the condition of IT systems in an audited area.

Standards and criteria for performing an IT system audit in HEP d.d. include:

- HEP d.d. business strategy
- HEP d.d. business plans and programs
- HEP d.d. development strategy
- Implementation of legislation regarding IT
- Implementation of internal acts regarding IT
- Implementation of IT standards

In order to meet standards and criteria, when performing an IT system audit in HEP d.d. and other types of audits, the following procedures are used:

- Croatian internal auditing standards
- Internal auditing department ethics code
- HEP d.d. professional ethics code
- HEP d.d. internal auditing manual
- HEP d.d. guidelines for internal auditing
- HEP d.d. internal auditing methodology

The process of information system internal audit in HEP d.d. includes the use of adequate methods, procedures, techniques and different means, ways and forms of performing an audit, which enable internal auditors to ascertain the actual and objective state and provide a professional evaluation and internal audit results.

Just like any other internal audit within HEP d.d., information system internal audit is performed in four stages [12]:

1. Internal audit planning
2. Information testing and evaluation
3. Reporting on internal audit results
4. Follow-up on implementation of results, recommendations and corrective activities.

In the stage of internal audit planning the following activities are carried out:

- drawing up an IT internal audit draft
- drawing up an IT internal audit action plan (internal audit scope, objectives, tasks)
- collecting information, data, analyses, reports on company's activities etc.
- collecting information on previously conducted internal audits
- compiling work documentation (schemes, analyses, flow-charts, test for conducting an internal audit etc.)
- sending announcement letters about performing an information system

internal audit (Resolution on performing an internal audit) and
- preparing activities in the field.

In the stage of information testing and evaluation the following activities are carried out:
- internal system controls assessment
- evaluating whether business activities are in line with legislation and HEP d.d. internal acts (compliance testing)
- evaluating alignment with standards (ISO 17799 and ISO 27001)
- performing tests using CAAT's tools, collecting evidence and defining results
- communicating with the management of the audited area during the audit and
- compiling work documentation.

In the stage of reporting on internal audit results the following activities are carried out:
- at the final meeting with the management of the audited area (auditee) all relevant results, recommendations, suggestions and corrective activities are presented in order to eliminate observed irregularities and implement necessary control measures
- a report on information system internal audit is drawn up
- the report is sent to persons in charge, i.e. to the management of the audited area, as well as to persons in charge of that part of company's activities.

In the follow-up stage on monitoring the implementation of results, recommendations and corrective activities the following activities are carried out:
- internal auditors establish the adequacy, efficiency and timeliness of control measures the management in charge implemented according to results, recommendations and corrective activities stated in the Internal Audit Report
- after receiving the Report the management in charge needs to take actions according to their accountability, make an action plan and notify the person in charge in the internal audit department
- the management of the audited area (auditee) is responsible for implementing and applying all of the auditors' recommendations and corrective activities.

According to place, time and tasks, the internal audit process is divided into:
1. Pre fieldwork activities
2. Fieldwork activities and
3. Post fieldwork activities

Pre fieldwork activities include: defining objectives and tasks of the audit, collecting information on audited department's activities, audit planning (drawing up a draft, an action plan and schedule), writing announcement letters – communicating with the report user and the management, preparing work documentation – risk assessment, defining objectives and tests for performing the audit).

Fieldwork activities include: communicating with the management of the audited area or department, testing and assessing information, performing tests, collecting relevant evidence, establishing findings and presenting the main audit findings or results to the management of the audited area or department (audite).

Post fieldwork activities include: writing the audit report, communicating with user of the internal audit report (auditee management), presenting the report to the auditee management and monitoring the implementation of agreed activities.

5. Conclusion

In this paper, it is highlighted a problem of uncontrolled investment in IT without clear benefits and influence on business strategy and business objectives achievement. Some models (COSO, CobIT, IT Balanced Scorecard…) for solving this problem are described, as well as, the way of using them as an interrelated models, and as a base for Internal Audits based on risk approach. In that way, it is possible to check periodically the realization of objectives at all levels and in all domains (COSO and CobIT) through balanced set of measures (business and IT). It is a fundament for better alignment between business and IT.

One of the reasons why it is necessary to perform information system internal audits in companies is the fact that information system

integrity protection has become an important business issue in today's business conditions, when companies' core activities are becoming more tightly linked with their information systems.

IT internal audit provides us with more reliable and more accurate information on IT asset protection, data integrity maintenance, and according to internal audit results we recommend corrective activities, whose timely implementation will affect the improvement in the efficiency and effectiveness of company's activities, with the aim of accomplishing HEP d.d. policy goals.

Final result of IT internal audit is not a report by an internal auditor but its effects and a timely implementation of recommendations and corrective activities (added value) with the purpose of implementation business goals of HEP d.d. in its entirety.

In that way, as a part of controlling department in HEP d.d., internal auditing improves audited processes and the overall activities of HEP d.d.

6. References

[1] T.A. Byrd, B.R. Lewis, R.W. Bryan: The leveraging influence of strategic alignment in IT investment: An empirical examination, Information & Management 43, 308-321, 2006.

[2] K. Celuch, G.B. Murphy, S.K. Callaway: More bang for your buck: Small firms and the importance of aligned information technology capabilities and strategic flexibility, Journal oh High Technology Management Research 17, 187-197, 2007.

[3] CobIT Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, IT Governance Institute, 2007.

[4] R.M. Amato, Deloitte Accountants: Moving Forward with IT Governance and CobIT, Eurocacs, 2008.

[5] ESB: Governance Review, 2006.

[6] Ernst & Young: CobIT: Logical Access Testing, 2005.

[7] W.V. Grembergen, R. Saull: Aligning Business and Information Technology through the Balanced Scorecard at a Major Canadian Financial Group: its Status Measured with an IT BSC Maturity Model, Proceedings of the 34th Hawaii International Conference on System Sciences, 2001.

[8] Z. Krakar, M. Žgela, S. Tomić Rotim: CobIT – Framework for IT Governance, 2007.

[9] A.D. Chambers, G.M. Selim, G. Vinten: Internal Auditing, 1997.

[10] CIPFA The Chartered Institute of Public Finance and Accountancy: Computer Audit Guidelines, 1998.

[11] ISACA: CISA Review Technical Information Manual, 2006.

[12] B. Tušek, L. Žager: Priručnik za rad interne revizije u HEP-u, 2006.

[13] R. Weber: Information Systems Control and Audit, 1999.

[14] A.D. Chambers, G. Rand: The Operational Auditing Handbook, 2000