Standards and Frameworks for Information System Security Auditing and Assurance

Mario Spremic

Abstract: - **Most organizations in all sectors of industry, commerce and government are fundamentally dependent on their information systems (IS) and would quickly cease to function should the technology (preferably information technology – IT) that underpins their activities ever come to halt [15]. The IT developments may have enormous implications for the operation, structure and strategy of organizations. IS and IT may contribute towards efficiency, productivity and competitiveness improvements of both inter-organizational and intra-organizational systems [1]. Successful organizations manage IT function in much the same way that they manage their other strategic functions and processes. This in particular means that they understand and manage risks associated with growing IT opportunities as well as critical dependence of many business processes on IT and vice-versa. IT risk management issues are not only any more marginal or 'technical' problems and become more and more a 'business problem'. Therefore, in this paper a Corporate IT Risk Management model is proposed and contemporary frameworks of IT Governance and IS Audit (CobiT, ISO 27000 'family', ITIL) is shown and explained.**

Key-Words: **IT Governance, IS Audit, Corporate IT Risk Management Model, CobiT**

I. INTRODUCTION

As the organizations are becoming increasingly dependent upon information systems (IS) and underlying information technology (IT) in order to achieve their corporate objectives and meet their business needs, the necessity for implementing widely applicable IS best practices standards and methodologies, offering high quality services is evident. The issue of managing the IT risks becomes less and less a technical problem, and more and more the problem of the whole organization i.e. a 'business problem' and many companies nowadays formally nominate executive directors for such activities [17].

IT Governance is the process for controlling an organization's IT resources, including information and communication systems and technology [8]. According to the IT Governance Institute [10], IT governance is the responsibility of executives and board of directors, and consists of leadership, organizational structures and processes that ensure that enterprise's IT sustain and extends the organization's strategies and objectives. The primary focus of IT governance is on the responsibility of the board and executive management to control formulation and the implementation of IT strategy, to ensure the alignment of IT and business, to identify metrics for measuring business value of IT and to manage IT risks in an effective way in order to ensure the fusion of business and IT [17].

IT risks, on the other hand, are risks associated with intensive use of IS and IT to support and improve business processes and business as a whole. They are related to threats and dangers that the intensive use of IS and IT may cause undesired or unexpected damages, misuses and losses in whole business model and its environment. Since the efficiency, effectiveness and in a great deal the successfulness of all business activities depend on the functioning of the IT and IS, a sound risk management process should not only include technical or operational issues but also executive management' frameworks such as IT Governance and IS Audit.

In this paper we particularly stress the importance of IT risk management policies and information security standards and assurance frameworks such as CobiT, ISO 27000, PCI DSS, Basel II, etc. Comprehensive Governance, Risk, Compliance (GRC) model proposed in the paper may be the useful tool in managing IT risk level. The very basis of the GRC model lies upon the IS Audit activities, namely upon thorough IT risk level assessment which give a level of assurance that certain IT processes are conducted in proper way.

II. NEW PERSPECTIVES ON IT RISKS MANAGEMENT

IT Risks represent the likelihood that in certain circumstances a given threat-source can exercise a particular potential vulnerability and negatively impacts the IS assets (data, software, hardware, etc.), IS services and technology and key business processes or the whole organization [17].

IT Risks = F (asset, threat, vulnerability)

Methodologies for assessing IT risks level may be qualitative and quantitative. Wide range of different evaluation models may be used, but methodologies have to be aligned with IT Governance rules, policies and procedures, and their main objective have to be to evaluate possible impact of a threat on the business and assess the risk level.

Quantitative risk assessment might be drawn upon methodologies used by financial institutions and insurance companies. By assigning values to information, systems, business processes, recovery costs, etc., impact, and therefore risk, can be measured in terms of direct and indirect costs. Quantitative risk can be expressed as Annualized Loss Expectancy (ALE). ALE is the expected monetary loss that can be expected for an asset due to a risk being realized over a one-year period.

$$ALE = SLE * ARO$$

where:

Mario Spremic is professor at the University of Zagreb, Faculty of Economics and Business. He can be reached at mspremic@efzg.hr

SLE (Single Loss Expectancy) is the value of a single loss of the asset. This may or may not be the entire asset. This is the impact of the loss.

ARO (Annualized Rate of Occurrence) is how often the loss occurs. This is the likelihood or the number of occurrences of the undesired event.

Therefore, if a company faces a 10.000€ loss due to the web site downtime, and if it happens in average 5 times a year, than the Annualized Loss Expectancy (ALE) is 50.000€. This is a rough approximation of the ALE, but if the company insists on measuring the IT performances we may expect the proliferation of the numbers. It also means that the company may spend up to, for example 10.000€ at the minimum for implementation of solid control countermeasures

From IT Governance, IS Audit and IS Security perspective, IT risk management is the process of understanding and responding to factors that may lead to a failure in the authenticity, non-repudiation, confidentiality, integrity or availability of an information system. Information security program helps organization to measure the IT risk level and provides the management processes, technology and assurance to:

- allow businesses' management to ensure business transactions and information exchanges between enterprises, customers, suppliers, partners and regulators can be trusted (*authenticity and non-repudiation*),
- ensure IT services are available and usable and can appropriately resist and recover from failures due to errors, deliberate attacks or disaster (*availability*),
- ensure information is protected against unauthorized modification or error so that accuracy, completeness and validity is maintained (*integrity*),
- ensure critical confidential information is withheld from those who should not have access to it (*confidentiality*).

Although, IT risks characteristics dramatically change in recent decades, IT is still often mistakenly regarded as a separate organization of the business and thus a separate risk, control and security environment. While since 10 or 15 years ago an IT risk could cause minor 'technical' problems, today it may affect the corporation's competitive position and strategic goals. An attack on Amazon.com, for example, would cost the company $600.000 an hour in revenue and if Cisco's systems were down for a day, the company would loose $70 million in revenues [14], not to mention indirect costs and reputation risk. It is estimated[1] that IS downtime put direct losses on brokerage operations at $4.5 million per hour, banking industry $2.1 million per hour, e-commerce operations $113.000, etc. Also, Fortune 500 companies would have average losses of about $96.000 per hour due to the IS downtime[2].

Therefore, Corporate IT Risk Management Model (CITRM) should be a holistic and structured approach that aligns governance policies, business strategy, management procedures, business processes and operational activities with the purpose of evaluating and managing risk and uncertainties the organization faces. The main objective of CITRM model is to align IS resources, IT infrastructure and business processes with governance policies and management procedures in order to effectively manage IT risk exposure. This in particular means that executive management and Board members become responsible for managing risk associated with using IS and IT in conducting business operations and transactions. Such initiatives are well known 'heritage' of certain regulatory framework (for example, Sarbanes-Oxley act or Basel II framework) and represent the core of IT Governance concept.

The fundamentals of the Corporate IT Risk Management Model are:

1. ***Corporate governance policies for managing IT risks*** – policies that are mandatory at all corporate levels and approved by the highest corporate bodies (Board, executive management). Typical examples are:
   - defining the 'risk appetite' which commonly represent the corporate rules and policies for IT risk response strategies (key metrics, Key Risk Indicators - KRIs, Key Performance Indicators - KPIs). This in particular means that the corporation have to define acceptable level of IT risks as the level of IT risk which will not affect organisation performance.
   - Corporate policies for analyzing the impact IT risks may have on the business (quantitative or qualitative measures for conducting a business impact analysis – BIA, metrics for IT risk validation, IT risk portfolio).
   - Accountability for IT control activities and framework for the IT risk reports (the dynamics of IT risk reports, who and to whom IT risk reports should be presented).
   - Establishing committees and other corporate 'bodies' responsible for managing IT risks (Audit Committee, IT Governance Committee).
   - Strategies for regulatory compliance and adopting industries best practices.

2. ***Procedures for managing IT risks on business units level or functional level.*** They represent the standards, guidelines and activities which help in implementation of corporate IT Governance policies (for example, IS Security Policy, Business Continuity Plan, etc). According to the regulatory requirements and specific area of interest, this usually means the adoption of world-wide standards or frameworks (CobiT, ISO 27001, Sarbanes-Oxley, Basel II, ITIL, SANS, SAS 70, …). Periodic internal or external IS audits are needed to detect the level of compliance with standards and regulatory frameworks. Performing IS audits are necessary in order to detect the priority risk areas, to identify specific IT controls needed, to constantly measure the level of their efficiency and to calculate IT risk level on regular basis.

3. ***Operational (technical) activities***, 'driven' by governance policies and management procedures

[1] Hiles, A. (2004): Business Continuity: Best Practices - World-Class Business Continuity Management 2nd ed., Disaster Center Bookstore, USA.
[2] Ibidem.

represent the counter-measures, which aim to raise the level of ‘immunity’ on threats or attacks to IT assets. Typical examples of operational IT controls include access controls, application controls, system controls, change controls, data accuracy controls, integrity controls, business continuity controls, etc.

III. THE CONCEPT OF IS ASSURANCE AND IS AUDITING

Managing risks is a cornerstone of IT governance, ensuring that an enterprise’s strategic objectives are not jeopardized by IT failures. IS assurance refers to the process of measuring the level of IS quality which in particular means measuring the level of the selected IT risks. This is doing by testing the level IT controls efficiency (for example, the more IT controls are effective, vulnerability is lower and opposite). Information system auditing process is associated to the process of assessing the level of IT risks. So, this is the clear connection between the control, quality (assurance) and audit ‘triangle’.

A good, or rather, inevitable approach for managing IT risks include thorough audit and quality assessment (assurance) of all aspects of IS and IT, including hardware, software, data, networks, organization and key business processes. The primary goal of the information system audit is to identify the key business processes that depend on IS and IT, to systematically and carefully examine their IT controls efficiency, to identify key risk areas and constantly measure the risk level, to warn about possible failures, as well as to offer suggestions to the executive management how to improve current IT risk management practices [17].

In order to provide a successful protection against possible misuses, an organization should develop methods and techniques for the control of the IT incidents and for identification of possible risk evaluation methods. *An IT Risk Management plan* should have following important steps:

1. IT risk identification and classification,
2. IT risk assessment (Business Impact Analysis) and priority determination,
3. IT risk responses strategies – identification of IT controls,
4. implementation and documentation of selected counter-measures (IT controls),
5. portfolio approach to IT risks and alignment with business strategy,
6. constant monitoring of IT risks level and auditing.

A. IT Risks Identification and Classification

Perhaps the most difficult aspect of process of managing risks is their identification and classification. IT risk identification process represent not only a listing of expected negative outcomes, but also their classification according to a proposed corporate framework and preparation for their assessment by evaluation of their possible impact on business, categorization of causes and triggers to the risk event, the probability of occurrence and the allocation of the responsibility for the risks. Generally, risks are identified in terms of their relevance to the specific business objectives or impact on business processes.

Some common frameworks or industry standards can help organizations to identify and classify IT risks. Apart from industry or country specific risk and regulatory frameworks (for example, Basel II, PCI DSS, Sarbanes-Oxley), in understanding where IT risks exist within the organization, a classic hierarchical risk approach should help (corporate or company-level IT risks, process-level IT risks – IT general risks and specific IT risks - IT applications and IT services risks).

B.IT Risks Assessment And Priority Determination

The objective of this step is to assess the important characteristics of IT risks such as ‘gravity’ and frequency. IT risks gravity is the measure of the damage or potential loss that certain undesired or unexpected activity may cause and commonly it can be expressed in financial terms. According the corporate governance polices, for all identified risks, *IT risk assessment plan* includes following activities:

- identification of the threats to IT resources and the exposure of IT infrastructure to various malicious or accidental acts,
- evaluation of the vulnerabilities to identified IT risks,
- determination of the IT risks probability of occurrence (frequency),
- evaluation of the business impact of IT risks occurrence (severity),
- analysis of the IT risks frequency and IT risks ranking (an example is given in table 1.),
- calculation of the IT risks ‘gravity’ and expected value of IT risks (an example is given in table 2.), and
- preparation for the response strategies and for the control of IT risks level.

Table 1. Example of analysis of IT risk drivers frequency and severity

IT risk scenario	**Risk drivers for frequency**	**Risk drivers for severity**
Authorized users perform illegal activities (confidentiality)	- Users with access to sensitive application functions - Lack of supervisory control - Improper definitions of access permissions - Excessive use of supervisory activities	- Inadequate monitoring of - system exception reports - Lack of management control - Lack of audit review - Inappropriate security policies
System and services disruption (availability)	- Number of potential damaging incidents that could cause a disruption of service - Susceptibility of hardware and software to damage	- Inability to correctly identify the impact of conditions that can result in disruption - Failure to develop

		and implement incident detection and escalation procedures - Failure to monitor for events that can result in a disruption of service
IT Project implementation failure (financial risk)	- Number of projects - Quality of defined program and project management approach	- Amount of project budget - Number of critical projects - Methods for evaluating project feasibility (ROI)

Table 2. Example of the IT risk assessment and priority determination activities

IT risk scenario	**Potential damage**	**Potential loss (BIA)**	**Risk ranking**
Authorized users perform illegal activities (confidentiality)	Users have unauthorized access to data, they can view and change them, they can manipulate with the system	100.000 €	Medium
System and services disruption (availability)	Disruption of key business processes and potential loss of important data	500.000 €	High
Incomplete transaction processing (integrity)	Financial reports may be incorrect, decision making process questionable	250.000 €	High
IT Project implementation failure (financial risk)	IT project not finished on time, costs to high, quality poor (Service Level, low functionality)	300.000 €	High

C. Strategies For IT Risks Responses – Identifying IT Controls

Once the organization has identified, classified and according to the business impact analysis (BIA) assessed IT risks, risk owners and 'affected' process owners are to be identified, appropriate responses should be developed and specific cost-effective controls over those risks should be designed. IT risk responses have to be align with IT Governance policies and may include following strategies:

- *acceptance* – the organization chooses to live with the risk and to constantly monitor its level (gravity and impact on the business and business processes),
- *reduction* – the organization takes steps to reduce the impact (gravity) or the probability of the risk occurrence,
- *avoidance* – the organization chooses to fully or partially avoid the risk,
- *sharing* – the organization transfers the risk by, for example, purchasing insurance, outsourcing risk management services, or engaging in partnership(s) regarding the risk management process to fully or partly cover risk exposure (especially in business continuity and disaster recovery plans).

Strategies for IT risks responses usually means that specific IT controls need to be implemented and their efficiency constantly monitored. *Control activities* are the policies, procedures and practices that are put into place so that business objectives are achieved and risk mitigation strategies are carried out. Control activities are developed to specifically address each control objective to mitigate the risks identified. An *IT control objective* is a statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity [10]. When conducting IS Audits, IS Auditors commonly perform test of IT control's efficiency using specific metrics (for example, RTO, RPO for business continuity process), maturity models and audit tools (CAATs, ACL software, etc.). Common metrics for testing the efficiency of business continuity plan may be:

- *MTBF* (Mean Time Between Failures) represents an important system characteristic which help to quantify the suitability of a system for a potential application. MTBF is the measure of the systems' functionality and service level. MTBF is often connected to the Mean Time to Repair (MTTR). ITPI [13] reported that high IT performers know that 80% of all outages are due to the change, and that 80% of mean time to repair (MTTR) is spent to figure out what changed.
- *Availability* represents the percentage of time when system is operational (for example, 99% availability means that the system downtime is 3,65 days per year, while 99,99% availability rate means that the downtime is 52 minutes per year).
- *First Fix Rate* - measures the percentage of incidents that successfully restored on the first fox attempt. It is leading indicator of system availability and MTTR; that is, how well an IT organization manages First Fix Rate will also result in radically improved MTTR and MTBF. First Fix Rate is commonly used in connotation of the service desk, where it measures how often the incident is resolved at the first point of contact between a customer and the service provider.
- *RTO (Recovery Time Objective)* - the period of time within which systems, services, applications or functions must be recovered after an outage. It is a maximum tolerable length of time that an IT infrastructure can be down after a failure or disaster occurs. The RTO is a

function of the extent to which the interruption disrupts normal operations and the amount of revenue lost per unit time as a result of the disaster.

- *RPO (Recovery Point Objective)* – the maximum amount of data loss an organization can sustain during an event. It is also the point in time (prior to outage) in which systems and data must be restored to. There is a growing in certain businesses (especially information intensive industries such as financial services) for RTO and RPO to be close to zero. The convergence of RTOs and RPOs to zero will result in exponential cost increase, thus corporate managers together with CIOs (Chief Information Officers) and CTOs (Chief Technology Officers) need to carefully balance these numbers and their costs.

D. IS Auditing Standards And Frameworks

Implementing IT Governance and IS Audit frameworks may help organizations manage IT risk level. In recent years various groups have developed world-wide known IT control frameworks and guidelines to assist management and auditors in developing optimal controls systems. Contemporary IT governance and IS audit frameworks are:

- *CobiT* (Control Objectives of Information and related Technology),
- *ISO 27000 standard* (ISO 27001:2005, ISO 27002:2005),
- *Basel II, ITIL, NIST, SANS, ISC2, etc.*

Developed by ISACA (Information System Audit and Control Association, www.isaca.org) and ITGI (IT Governance Institute, www.itgi.org), **CobiT** is the most widely accepted IT governance framework, organized by key IT control objectives, which are broken into detailed IT controls. Current version 4.1 of CobiT divides IT into four domains (Plan and Organise, Acquire and Implement, Deliver and Support, and Monitor and Evaluate), which are broken into 34 IT processes (or IT control objective) covering all important processes within IT, and then further divided into more than 300 detailed IT controls. Therefore, CobiT provide a sound support especially for company-level and process-level IT risks management. For each IT control objective CobiT defines:

- performance goals and metrics (for example, RPO, RTO, availability time),
- KRI (Key Risk Indicator), KPI (Key Performance Indicator)
- maturity models (0-5 scale) to assist in benchmarking and decision-making for process improvements,
- a RACI chart identifying who is Responsible, Accountable, Consulted, and/or Informed for specific IT control objective.

CobiT processes of particular interest for information security issues may be DS 4 (Ensure Continuous Service) and DS 5 (Ensure System Security) with wide range of sub-controls useful for modelling control environment. CobiT represent an 'umbrella' framework for implementing IT Governance policies and procedures. It is a broad and comprehensive de-facto standard which comprises all activities, processes and services an IT organization need to manage (or rather govern). Therefore, when engaging in IT Governance activities it is inevitable to use CobiT framework to in details analyse the alignment of current IS and supporting IT infrastructure and business requirements towards it.

If CobiT-based information system audit or any further 'due diligence' come up with the conclusion that an IT organization underperforms in a specific area, an additional project may be opened to assure the compliance and alignment with business requirements. For example:

- **ITIL** framework may be used to assure better **IS service delivery and service management**,
- **Val IT** framework may be used to assure efficient management of **IT investments** which may result with additional business value,
- **ISO 27001** standard and **SANS** (www.sans.org), **NIST** (www.nist.org), **(ISC)2** framework (www.isc2.org) and **PCI DSS** (www.pcisecuritystandards.org) may be used to manage the level of **IT security risks**,
- **Prince 2** and/or **PMBOK** may be used to bridge the gap in **IT project management** activities,

ISO/IEC 27000:2005 (The Code of Practice for information Security Management) is the series of standards (ISO 27000 – ISO 27008 with a number of guidelines) associated with managing information security. ISO 27001:2005 consists of 10 control or risks areas in which about 40 major and 128 detailed IT security controls are offered.

The **PCI DSS** (Payment Card Industry Data Security Standard) is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data and manage IT security and privacy risk in credit card transactions. PCI DSS has 12 requirements (IT control objectives) and more than 50 recommended IT controls.

By adopting industry best practices (e.g. CobiT, ISO 27000, PCI DSS) and adjusting IT infrastructure with high-level executive objectives, companies can lower IT risks, especially security and operational risks. According to the recent IDC white paper[3] implementation of comprehensive IT Governance and IS auditing standards downtime risks my be lower by up to 85%, heavily reducing interruptions to daily data processing and access and supporting business continuity.

The possible results of comprehensive efforts (possible implementation of CITRM model) in managing IT risk are presented in table 3. IT Governance and IS Audit activities there may give a clear guideline to executive management in managing IT risk.

[3] IDC White Paper (2009): Reducing Downtime and Business Loss: Addressing Business Risk with Effective Technology, IDC, August 2009.

Table 3. The results of Corporate IT Risk Management Model implementation

Key business process	Sales orders (e-orders)
IT risk	System disruption
IT risk level	High – critical, loss of data, corporate risk
Potential loss (BIA) (per day)	500.000 €
IT Risk Response Strategy	Immediate action, risk level reduction
IT (governance) goal	Number of hours lost per user per month due to unplanned outages
IT Control	CobiT 4.1. (*DS4, DS5)* ITIL *BCM* ISO 27001 (10, 11, 4)
Key Metrics – IT Control Efficiency	Availability = 99,95% RTO < 3h RPO < 3h First Fix Rate > 90% MTTR < 30 minutes MTBF < 20 minutes
Detailed IT metrics	- Percent of availability service level agreements (SLAs) met - Number of business-critical processes relying on IT that are not covered by IT continuity plan - Percent of tests that achieve recovery objectives - Frequency of service interruption of critical systems
Responsible person (process owner)	XY

IV. CONCLUDING REMARKS

Although, traditionally, only the IT departments were responsible for managing IT risks, their importance affects the fact that the number of companies starting to systematically deal with such problems is ever increasing. The issue of managing the IT risks becomes less and less a technical problem, and more and more the problem of the whole organization i.e. a ‘business problem’ and many companies nowadays formally nominate executive directors for such activities. Therefore, we find the proposed corporate IT risk management (CITRM) model incorporating contemporary IT governance and IS audit issues suitable and inevitable framework for managing IT risk in today’s business.

Plans for future researches include testing the Corporate IT Risk Management model on wide range of companies from various industries. Also, it may be of particular interest to find out is the model suitable for all industries. The difficulties may arise from the fact that the companies in general are not so willing to participate in such researches, case studies or in-depth interviews because they may reveal some vulnerabilities in their businesses and expose to the certain risk.

References

[1]. Brynjolfson, E. and Hitt, L.M. (1993)*: Is information systems spending productive? New evidence and new results*, Proceedings of the International Conference on Information Systems,Orlando, FL, pp. 47-64.

[2]. Buhalis, D., (2004): eAirlines: strategic and tactical use of ICTs in the airline industry, Information & Management, 41, pp. 805-825

[3]. Champlain, J.J. (2003): Auditing Information Systems, 2nd ed. John Wiley & Sons, SAD.

[4]. COSO (2004), *Enterprise Risk Management Integrated Framework*, September, 2004, www.coso.org7publications.htm, accessed, January, 2008.

[5]. Gartner (2002): ‘The Elusive Business Value of IT’, August 2002.

[6]. Groznik, A., Kovačič, A., Spremić, M., (2003): Do IT Investments Have a Real Business Value?, *Applied Informatics*, No. 4, 2003, pp. 180-189.

[7]. Hiles, A. (2004): Business Continuity: Best Practices - World-Class Business Continuity Management 2nd ed., Disaster Center Bookstore, USA.

[8]. Hunton, J.E., Bryant, S.M., Bagranoff, N.A.: (2004): Core Concepts of Information Technology Auditing, John Wiley &Sons Inc., SAD.

[9]. International Organization for Standardization (ISO), *Code of Practice for Information Security Management*, ISO/IEC 17799, Switzerland, 2005

[10]. ITGI (2003): *Board Briefing on IT Governance*, 2nd ed., IT Governance Institute, Rolling Meadows, Illinois, SAD.

[11]. ITGI (2007): *IT Control Objectives for Basel II – The Importance of Governance and Risk Management for Compliance*, IT Governance Institute, Rolling Meadows, Illinois, SAD.

[12]. ITGI and PricewaterhouseCoopers (2006): *IT Governance Global Status Report,* IT Governance Institute, Rolling Meadows, Illinois, SAD.

[13]. ITPI (2006) IT Process Institute: Reframing IT Audit and Control Resources Decisions, 2006,www.itpi.org, accessed April 2008.

[14]. Nolan, R. and McFarlan, F.W., (2005): Information Technology and Board of Directors, Harvard Business Review, October, 2005.

[15]. Peppard, J., Ward, J., (2004): Beyond strategic information systems: towards an IS capability, Journal of Strategic Information Syatems, 13 (2004), pp. 167-194.

[16]. Plummer, D. (2006): IT Must Think Differently, Act Differently to Drive Business Growth, Gartner Symposium/IT Expo, October 2006.

[17]. Spremic, M. **(**2009): IT Governance Mechanisms in Managing IT Business Value, WSEAS Transactions on Information Science and Applications**,** Issue 6, Volume 6, June 2009, pp. 906-915

[18]. Symons, C., (2005): IT Governance Framework: Structures, Processes and Framework, Forrester Research, Inc.

[19]. Tam K. Y.: The Impact of Information Technology Investments on Firm Performance and Evaluation: Evidence form Newly Industrialized Economies. Information Systems Research, 9, 1, 1998, pp. 85-98.

[20]. Van Grembergen, W., De Haes, S., (2005): Measuring and Improving IT Governance Through the Balanced Scorecard, Information System Control Journal, Volume 2, 2005.

[21]. Weill, P., Ross, J.W., (2004): IT Governance: How Top Performers Manage IT Decision Rights for Superior Results, Harvard Business School Press, 2004.