IT Governance Mechanisms in Managing IT Business Value

MARIO SPREMIĆ
Faculty of Economics and Business Zagreb, University of Zagreb
Kennedy's sq 6, 10000 Zagreb
CROATIA
e-mail: mspremic@efzg.hr

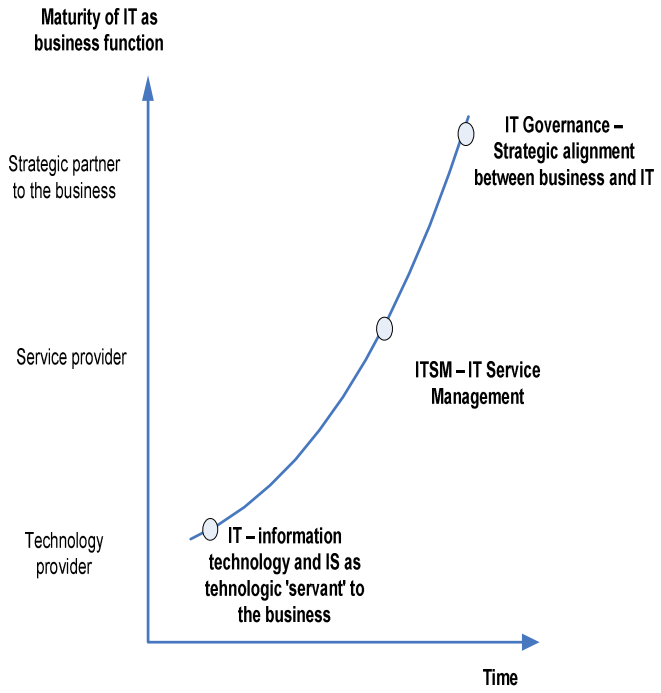
Abstract: Most organizations in all sectors of industry, commerce and government are fundamentally dependent on their information systems (IS) and would quickly cease to function should the technology (preferably information technology – IT) that underpins their activities ever come to halt [15]. The development and governance of proper IT infrastructure may have enormous implications for the operation, structure and strategy of organizations. IT and IS may contribute towards efficiency, productivity and competitiveness improvements of both inter-organizational and intra-organizational systems [1]. The business value derived from IT investments only emerges through business changes and innovations, whether they are product/service innovation, new business models, or process change. In this paper a newly concept of IT Governance and its mechanisms are explained in further details. 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 can be seen as a structure of relationships and processes to direct and control the enterprise use of IT to achieve the enterprise's goals by adding value while balancing risk vs. return over IT and its processes. While IT management is mainly focused on the daily effective and efficient supply of IT services and IT operations, IT governance is much broader concept which focuses on performing and transforming IT to meet present and future demands of business and the business' customers. IT Governance may be implemented using its key mechanisms such as business/IT strategic alignment, value creation and delivery, risk management (value preservation), resource management and performance measurement. In this paper key analytical IT Governance mechanisms such as information system audit and IT risk management are explained in further details.

Key-Words: IT Governance, Information System Audit, CobiT

1. Introduction: Governing IT is a business not a 'technical' problem

In the early days of implementing IT in the business, it was often seen as a technical support function and was typically managed by finance departments. When evolving from technology providers into strategic partners, IT organizations typically follow a three-stage approach. Each evolutionary stage builds upon the others beginning with *IT infrastructure management* (ITIM). During this stage, the IT's role in the organizations focus on improving the management of the enterprise (technological) infrastructure. Effective infrastructure management mainly is associated with maximizing return on computing assets and taking control of the infrastructure, the devices it contains and the data it generates [10]. The next stage, *IT service management* (ITSM), sees the IT organizations actively identifying the services its customers need and focusing on planning and delivering those services to meet availability, performance, and security requirements. In addition, IT contributes to the businesses by managing service-level agreements, both internally and externally, as well as by meeting agreed-upon quality and cost targets. Ultimately, when IT organizations evolve to *IT business value management* (*IT Governance*), they are transformed into true business partners enabling new business opportunities [8]. In that stage, IT processes are fully integrated with the complete lifecycle of business processes improving service quality and business agility.

Figure 1. Evolvement of IT as corporate function



While early IT implementations were clearly focused on automation of clerical and repetitive tasks, in today's highly competitive business environment, effective and innovative use of information technology (IT) has the potential to transform businesses and drive stakeholder value [22], [15].

According to the recent ITGI-PricewaterhouseCoopers study results, IT is quite to very important to delivery of the corporate strategy and vision [11]. On the other hand, poorly managed IT investment or badly implemented IT projects will lead to value erosion and competitive disadvantage [4], [12], [23]. A number of or company–level studies and analyses show that IT contributes substantially to company's productivity growth. This contribution is by all means strong where IT strategy is linked with business strategy, thus IT can initiate major changes in organization structure, business processes and overall activities.

In one study, Brynjolfsson and Hitt [1] concluded 'that while computers make a positive contribution to productivity growth at the firm level, the greatest benefit of computers appears to be realized when computer investment is coupled with other complementary investments; new strategies, new business processes, and new organizations all appear to be important.' Central message from the research literature, and one that is universally accepted, is that technology itself has no inherent value and that IT is unlikely to be source of sustainable competitive advantage [15]. The business value derived from IT investments only emerges through business changes and innovations, whether they are product/service innovation, new business models, or process change.

IT Governance issues are not only any more marginal or 'technical' problems and become more and more a 'business problem'. Therefore, in this paper emerging issues in IT Governance are discussed and the mechanisms and methodologies for evaluating IT Business Value explained in further details.

2. Evolving the IT Governance model

A good theoretical path to IT Governance issues could be found in IT Strategy and IT/Business Alignment literature. Venkatraman [22], for example, illustrates the changes that occur in the perceived contribution of IT by the business during the transformation from Service Provider to Strategic Partner as presented in Table 1.

Table 1. IT as Service provider or as Strategic partner

Service provider	Strategic partner
• IT is for efficiency • Budgets are driven by external benchmarks • IT is separable from the business • IT is seen as an expense to control • IT managers are technical experts	• IT for business growth • Budgets are driven by business strategy • IT is inseparable from the business • IT is seen as an investment to manage • IT managers are business problem solvers

Van Grembergen [21] stands on that point, but also emphasizes the strategic potential IT initiatives could have if managed (or rather 'governed') properly. When engaging in those changes, IT becomes not only a success factor for survival and prosperity, but also an opportunity for differentiation and achieving competitive advantage[1]. This should undoubtedly be achieved by putting in place a management of IT that is service oriented (ITSM) and by establishing an IT Governance capable of aligning IT with the Enterprise Governance objectives.

3. Corporate Governance and IT Governance – literature review

In order to understand the concept of IT governance a detailed insight into the principles of corporate governance and its constituents is needed. In their

[1] Van Grembergen, W., (2004): *Strategies for Information Technology Governance*, Idea Group, 2004.

publications on measuring the performance of corporate boards, M.J. Epstein and M.J. Roy state that "governance concerns relate to practices of both corporate boards and senior managers" and "the question being asked is whether the decision-making process and the decisions themselves are made in the interest of shareholders, employees, and other stakeholders or whether they are primarily in the interests of the executives[2]." The corporate governance framework is there to encourage the efficient use of resources and equally to require accountability for the stewardship of those resources. The aim is to align as nearly as possible the interests of individuals, corporations and society[3].

IT governance concerns relate to IT practices of boards and senior managers. The question is whether IT structures, processes, relational mechanisms and IT decisions are made in the interest of shareholders and other stakeholders, or primarily in the executives' interests. IT governance closely relates to corporate governance, the structure of the IT organization and its objectives and alignment to the business objectives.

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. It is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives.

Van Grembergen [21] stands on that point and defined IT Governance as the organizational capacity exercised by the Board, executive management and IT management to control the formulation and implementation of IT strategy and in this way ensure the fusion of business and IT. 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. Nolan and McFarlan [14] recently pointed out that 'a lack of board oversight for IT activities is dangerous; it puts the firm at risk in the same way that failing to audit its books would'. There are several ways of looking at the similarities between corporate governance and IT governance, as described in literature ([21],[22],[14]). Van Grembergen et al. use Shleifer and Vishny's work ([6]) and stress three key questions that the management should address to display the connectivity between corporate governance and IT governance (table 2.).

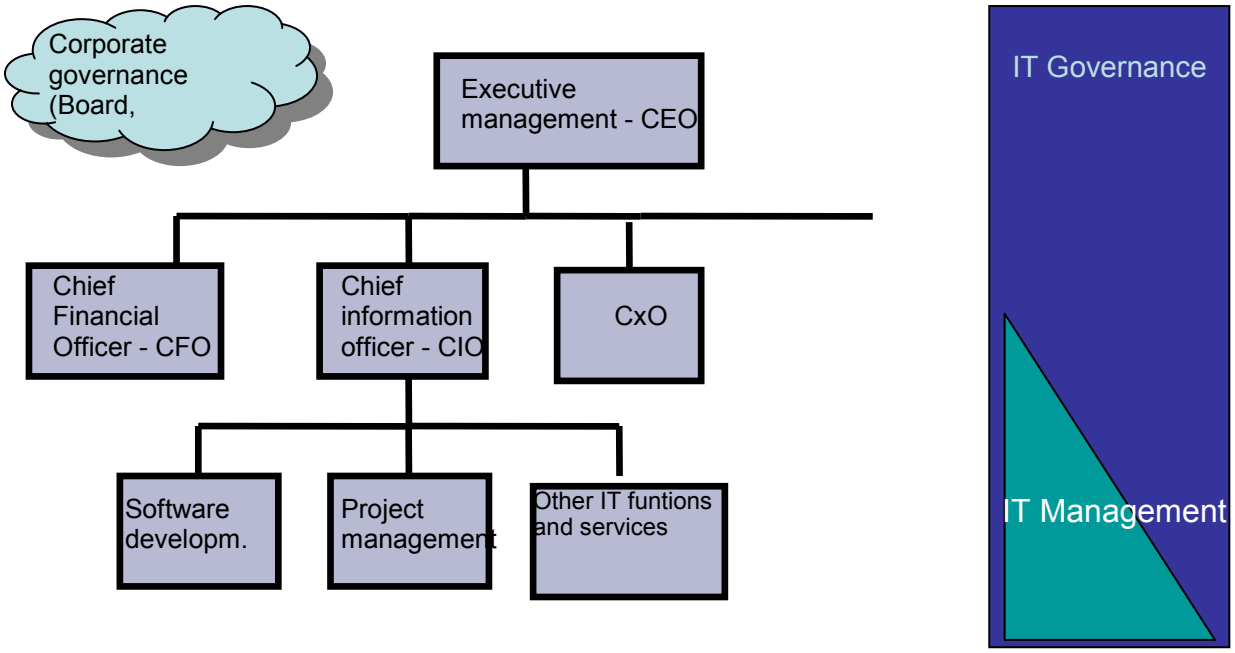
Table 2: Corporate and IT governance questions

Corporate Governance Questions:	**IT Governance Questions:**
How do suppliers of finance get managers to return some of the profits to them?	How does management get their CIO and IT organization to return some business value to them?
How do suppliers of finance make sure that managers do not steal the capital they supply or invest it in bad projects?	How does top management make sure that their CIO and IT organization does not steal the capital they supply or invest in bad projects?
How do suppliers of finance control management?	How does top management control their CIO and IT organizations?

Figure 2. shows a clear difference between IT governance and IT management. While IT management is mainly focused on the daily effective and efficient supply of IT services and IT operations, IT governance is much broader concept which focuses on performing and transforming IT to meet present and future demands of business and the business' customers. This in particular means that executive management members and corporate governance organizations bodies need to take responsibility for governing IT, which makes IT Governance a key executive function.

[2] Epstein, M.J., M.J. Roy, (2004): "How Does Your Board Rate?," *Strategic Finance*, February, p. 25-31, 2004.
[3] Sir Adrian Cadbury (2000): Global Corporate Governance Forum, World Bank, 2000.

Figure 2. Differences between IT Governance and IT Management concepts



3.1. IT Governance mechanisms

IT governance has primarily been driven by the need for the transparency of enterprise risks and the protection of shareholder value. The overall objective of IT governance is to understand the issues and the strategic importance of IT, so that the firm can maintain its operations and implement strategies to enable the company to better compete now and in the future. IT governance thus enables the enterprise to take full advantage of its information, thereby maximising benefits, capitalising on opportunities and gaining competitive advantage. Key IT governance mechanisms are [10]:

- Business/IT strategic alignment
- Value creation and delivery
- Risk management (value preservation)
- Resource management
- IS auditing and performance measurement.

Primarily of interest to business and technology management are the management guidelines - tools and mechanisms to help assign responsibility, measure performance, and benchmark and address gaps between actual and desired capability. The guidelines help provide answers to typical management questions:

- How far should we go in controlling IT, and is the cost justified by the benefit?
- What are the indicators of good performance?
- What are the key management practices to apply?
- What do others do?
- How do we measure and compare?

While in other papers [17] some mechanisms such as strategic alignment of business with IS and IT was explained, in this one we particularly stress the importance of analytical IT Governance mechanisms. For example, managing risks represent one of these mechanisms, ensuring that an enterprise's strategic objectives are not jeopardized by IT failures. On the other hand, performance measurement phase, as another IT Governance mechanism include audit and assessment activities which can create the opportunity to take time corrective measures, if needed.
So, the key IT Governance mechanism is thorough audit and quality assessment of all aspects of IS and IT, including hardware, software, data, networks, organization and key business processes.

4. Information System Audit as a key IT Governance mechanism

Managing business value represent a cornerstone of IT Governance, ensuring that an enterprise's strategic objectives are not jeopardized by IT failures. On the other hand, performance measurement phase intensively include audit and assessment activities which can create the opportunity to take corrective measures, if needed.

The primary goals of the information system audit (IS audit) are to [17]:
- identify the key business processes that depend on IT or IS,
- to systematically and carefully examine their controls efficiency,
- to identify key risk areas and constantly measure the risk level,
- to warn about possible failures, and
- to offer suggestions to the executive management how to improve current IT risk management practices.

This in particular mean that by engaging in IS auditing companies can periodically measure the IT performances using the well-proved, world-wide frameworks or methods such as CobiT, Risk IT, ITIL, ISO 27001, etc. Such tendencies are mostly motivated by specific regulatory pressures (for example, Sarbanes-Oxley act, Basel II framework, etc.), rather than by IT value-added initiatives.

In addition to the term of *information systems auditing*, the term such as *information technology auditing (IT Audit)* is often used. Regardless of different terms being used, the goals of the information systems audit are:
- to systematically, thoroughly, and carefully examine the controls within the business processes that are supported by information systems,
- to identify weak risk areas and to assess the risk level,
- to measure the overall IT performance according to the business requirements
- to warn about possible omissions and risks, and thus examine the quality of the company's information system.

Information system audit mainly refer to truly analytical part of IT Governance by which the level of IS performance can be measured and information system quality (IS quality) assessed. IS quality is a relative category which measures the current performance of the information system with ideal or required one. The more discrepancy of the actual performance of the information system to ideal (required) one, the system is of less quality and vice-versa. The required level of quality my be defined by regulation frameworks or should be stated in IS strategy or formulated with business objectives.

Actual level of information system quality need to be periodically reviewed by the systematic control activities and the level of its quality is assessed by IS audit. When conducting internal IS control activities companies engage in internal IS audit, while external IS auditing refers to auditing activities performed by external authority (specialised audit company, regulation authority such central bank).

In recent years various groups have developed world-wide known IT Governance and IS Audit frameworks and guidelines to assist management and auditors in developing optimal performance and controls systems. Contemporary frameworks are:
- *CobiT* (Control Objectives of Information and related Technology),
- Risk IT
- *ISO 27000 'family'* (ISO 27001:2005, ISO 27002:2005), and
- *ITIL* (IT Infrastructure Library)
- *VAL IT* framework.

4.1 CobiT - a generic methodology for Information System Audit and IT Governance

Developed by ISACA (Information System Audit and Control Association, www.isaca.org) and ITGI (IT Governance Institute, www.itgi.org), CobiT (Control Objective for Information and related Technology) is the 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 key IT processes, and then further divided into more than 300 detailed IT control objectives. For each of the 34 IT processes 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 process.

CobiT processes of particular interest for managing IT business value may be PO 1 (Define Strategic IT Plan), PO 5 (Manage IT Investment), PO 9 (Assess and Manage Risks), ME 1 (Monitor and Evaluate IT Performance) and ME 4 (Provide IT Governance). 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 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 27000 norm 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, etc.
- Risk IT framework may be used to help companies manage IT risks.

5. IT Risk Management as a key IT Governance mechanism

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

IT Risks = F (asset, threat, vulnerability)

There are quantitative and qualitative methods of assessing IT risks. Quantitative risk assessment draws 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. Mathematically, 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:

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 40.000€ at the minimum for implementation of solid control systems. Constant monitoring of the web site performance is crucial, while it may happen that the web sales grows significantly as well as that the SLE and ALE.

From IT Governance, IS Audit and IS quality 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. For example, 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[4] 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[5].

5.1. IT Risk Management Plan

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.

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

5.2. 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	• Inability to correctly identify the impact of conditions that can result in disruption

	disruption of service • Susceptibility of hardware and software to damage	•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)

This in particular means that risk analysts have performed a business impact analysis (BIA). Business impact analysis is an essential component of an organization's business continuity (BC) plan[6]. It is the management level process to prioritize business functions by assessing the potential quantitative (financial) and qualitative (non-financial) impact that might result if an organization was to experience a business continuity event[7]. BIA is a systematic process aimed to identify: key business processes performed by an organization, the resources required to support each process performed, the impact of failing of performing a process, the criticality of each process, a recovery time objective (RTO) for each process, recovery point objective (RPO) and availability rate for each process.

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

IT risk scenario	**Potential damage**	**Pot. 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

Classification of IT risks priorities are based on the probability of occurrence of each IT risks and their potential severity (the results of business impact analysis). According to the IT Governance policies and procedures one of most appropriate method for calculating IT risk level has to be defined and Board members and the executive managers need to approve it. Transparent and agreed risk management framework and clear rules and responsibilities for implementing it represent key cornerstones of effective IT risk management process. As mentioned previously, metrics for measuring IT risk level may be quantitative and qualitative. Quantitative metrics may be based on specific, even complex algorithms which executive managers use to quantify the risk level (for example: probability of occurrence multiply by risk severity). The simple algorithms may be improved according to the specific needs (the risk environment, business environment, regulatory requirements, etc.).

6. Conclusion

Although, traditionally, only the IT departments were responsible for managing IT initiatives, their importance affects the fact that the number of companies starting to systematically deal with such problems is ever increasing. As the organizations are becoming

[6] Business continuity plan (BCP) is a clearly defined and documented plan for use at the time of a Business Continuity Emergency, Event, Incident and/or Crisis (E/I/C). Typically a plan will cover all the key personnel, resources, services and actions required to manage the business continuity management (BCM) process, The Business Contiunity Institute (2002): Glossary of terms, www.thebci.org, accessed 12/2008

[7] The Business Contiunity Institute (2002): Glossary of terms, www.thebci.org, accessed 07/2007.

increasingly dependent upon IT in order to achieve their corporate objectives and meet their business needs, the necessity for implementing widely applicable IT best practices standards and methodologies, offering high quality services is evident. The issue of managing the IT 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.

In prior years, information technology (IT) had been viewed only as supporting player within overall company's strategy. Automation was, for example, limited to existing organizational function. But opinions have changed with the successful implementation of IT innovations and massive IT investments. Information system (IS), as well as IT in general, becomes extremely important asset that can strongly influence company market position, and which must be carefully monitored, controlled and planned. Improving the planning process for information systems is one of the key concerns for corporate management.

In this paper we argued about IT Governance concept and its mechanisms: business/IT strategic alignment, value creation and delivery, risk management (value preservation), resource management and IS auditing and performance measurement. Analytical IT Governance mechanisms such as IS auditing and IT risk management were discussed in further details. CobiT as a generic methodology for IT Governance was shown and explained. Apart from CobiT as an 'umbrella' methodology for IT Governance, a number of world-wide frameworks and methodologies used for measuring the performance of IT was mentioned (ITIL, Val IT, Risk IT, ISO 27001). Such tendencies, under the IT Audit 'umbrella', may help to measure the actual performance and quality of information systems and the business value of IT Governance initiatives.

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.] Spremić, M**.,** Žmirak, Z., Kraljević, K. (2008): Evolving IT Governance Model – Research Study on Croatian Large Companies, *WSEAS Transactions on Business and Economics***,** Issue 5, Volume 5, May 2008, pp. 244-253..

[18.] Spremic, M., Strugar, I. (2002): Strategic Information System Planning in Croatia: Organizational and Managerial Challenges, *International Journal of Accounting Information Systems*, Vol. 3, Num. 3, pp. 183-200.

[19.] Symons, C., (2005): IT Governance Framework: Structures, Processes and Framework, Forrester Research, Inc.
[20.] 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.
[21.] Van Grembergen, W., De Haes, S., (2005): Measuring and Improving IT Governance Through the Balanced Scorecard, Information System Control Journal, Volume 2, 2005.
[22.] Venkatraman, N., (1999): *Valuing the IS Contribution to the Business*, Computer Sciences Corporation.
[23.] Weill, P., Ross, J.W., (2004): IT Governance: How Top Performers Manage IT Decision Rights for Superior Results, Harvard Business School Press, 2004.