IT Risk Management in the Context of IT Governance: Theory vs. Practice

Artur ROT
Department of Management Information Systems Engineering
Wroclaw University of Economics
Wroclaw, Poland

ABSTRACT

Information Technology plays in a modern enterprise very significant role, appearing almost in every aspect of its business activity. It is proved i.e. by the amount of investments expenditures on these technologies which often take over half of all company’s investments’ expenditures. In many cases these expenditures do not bring assumed and desired effects. In such a situation there exists a need of systematized approach to effective application of Information Technology in the enterprise, with its aim to maximize value of the enterprise. One of possible solutions is implementation of IT Governance conception. Crucial element of IT Governance are such elements as management of IT security or connected to it issues of IT risk management. IS/IT Security, IT audit and IT Governance are permeating and correlative areas, crucial for functionality of IT in modern organizations. The aim of this article is to present selected issues from the area of IT risk management and IT security against a background of IT Governance concept. The paper will also present results of research concerning discussed issues in the practice of Polish enterprises.

Keywords: IT Governance, IT risk management, IT security, risk management practice, security management.

1. INTRODUCTION TO IT GOVERNANCE

There are not many companies which in everyday activity do not use Information Technologies. Support of business processes with information systems and technologies introduce new, previously not existed types of risks, which should be managed. In order to do it there appeared a new concept described as IT Governance. It constitutes integral component of corporate governance, defining rules, good practices and norms referring to broadly understood management of organization.

In the simplest way this concept is referred to such organization of company’s IT strategy, which harmonize with business strategy, ensuring to the company achievement of its goals and introducing good practices of risk management, and also in the measurement of IT performance. IT Governance, concentrates on the fact that business processes could bring measurable benefits and functionality of IT and what goes with it functionality of the whole enterprise took place according to the rule of risk minimizing. That is why problems of IT risk management are so crucial for discussed conception. In the subject’s literature there exist a few definitions of IT Governance, which the most important seems to be the one formulated by ISACA - The Information Systems Audit and Control Association, according to which IT Governance “constitutes of responsibility of supervisory board and management of the company that is integral part of corporate governance, including in it the elements of leadership, structures and processes of organization” [3] [8]. The second definition, very often quoted in the literature by P. Weill and J. Ross claims that IT Governance it is definition of decisive frames and availability of structure, assuring desired behaviors in IT. The next definition elaborated by W. van Grembergen says that, it is a concept of management, applied by organization, directed at supervision over IT portfolio. IT governance indicates outline of IT decisions distribution, creating rights and duties for different departments in organization, it manages rules and procedures for creation and monitoring decisions in strategic for Information Technology issues [8].

The most important areas of IT Governance are: IT strategy, risk management, resources management and performance measurement. The same like in the case of corporate governance, the basic aim of IT Governance is maximization of benefits and values of organization and minimization of different types of risk, which results from application of modern Information Technologies in enterprises [9].

IT Governance is very often understood as a code of good practices in the management of Information Technology. Therefore IT Governance it is not only the same technologies, but most of all sequence of guidelines, rules, practices connected with management of information and many non technical ventures at the strategic level e.g. personnel management. Application of clear rules of IT Governance builds confidence and shows that IT does not generate excessive business risk and gives greater probability of business plans achievement. Thanks to application of IT Governance mechanisms the greatest degree possessed information
and applied technologies and maximize resulting from it business benefits. Research conducted in enterprises show that companies possessing the most advanced solution in the scope of IT Governance have 20% better profitability in comparison to companies from the same sector and having similar strategies, but having weakly developed IT Governance. What is more, researches prove that efficacy of investments in the area of Information Technologies in these first companies is about 40% higher [4]. There should be underlined that IT Governance should not only be associated with activity of IT departments and it is not the concept of its management. It cannot be identified with such famous standards as ITIL or COBIT, which are very useful and helpful methodologies in implementation of this concept.

2. MAIN AREAS OF IT GOVERNANCE

Discussed concept embraces succession of areas of enterprise’s functionality and used Information technologies. As its main points there can be mentioned: strategic adaptation of business and applied in it Information Technologies, generation of values thanks to applied IT tools, effective application of information resources, security management and what is strictly connected with it - IT risk and performance measurement. As it was mentioned the crucial area of IT Governance are rules and practices in the scope of security management or connected with it problems of IT risk management. Main areas and rules of IT Governance can most of all include [8]:

- **Strategic adaptation of business and IT** – concentration on the issue that both areas should mutually realize strategy of organization. Appropriate adaptation of business and applied Information Technologies may happen only when the employees from both areas communicate effectively in the issues of planning, costs and effects.

- **Increasing value** – the main measure of Information Technology value are i.e. appropriately realized supplies of products or provision of services on time, in assumed budget, in appropriate quality achieving assumed benefits; competitive advantage, customers’ satisfaction, acceleration of entrance on market, shortened time of orders realization, increased productivity of employees, better profitability etc.

- **Management of resources** – the key to high IT efficiency are optimal investments and the best usage of possessed information resources in the process of service provision for business. Both new investments and expenditures for current activity in the range of Information Technologies must be adapted to the needs resulting from the strategy accepted by enterprise.

- **IT risk management** – this area includes different types of risk connected with application of Information Technology in the enterprise, i.e. protection of information resources, data recovery after failures or ensuring continuity of operation. In order to manage Information Technology risk effectively the management of the company has to understand, what is the attitude of the enterprise to the risk, they must be aware of existence of wide spectrum of threats and know legal and regulating requirements, they should also be aware of main types of Threats and their responsibility for it.

- **Measurement of IT effectiveness** – it consists of tracking the realization of information ventures and monitoring the process of Information Technology services provision. The most important measures is participation of expenditures on IT in the revenues, participation of expenditures on IT operation activity in total amount of expenditures on these technologies, the amount of expenditures on Information Technologies in calculation for one employee, number of computers for one employee, participation of software maintenance costs in the total costs of expenditures on IT. They are objective measures, although much more important are subjective measures which are very hard to measure. They enable measure of business needs i.e. functionality, quality, cost effectiveness. The examples of such measures are i.e.: availability, reliability, security, functionality, level of quality, adaptation to business needs etc.

Summing up, there can be stated that the main rules of IT Governance are analysis, how Information Technology provides values in starting new business processes, improve effectiveness of existing processes and of the whole organization and supports risk management, manages information security and ensures legality.

As it was stated at the beginning, the basic elements of IT Governance are also problems connected with management of Information Systems security or strictly connected with it problems of IT risk management. Information technology security, audit and IT Governance are permeating and strongly correlative areas, crucial for functionality of Information Technologies in contemporary enterprises and therefore for organizations itself.

3. IT RISK MANAGEMENT AS AN ELEMENT OF IT GOVERNANCE

As organizations become more and more dependent on their computer-based information systems, which play a vital role and important part in their business operations, there needs to be a greater awareness and concern about the security of these systems. Information has become the
key resource of many organizations. Information security appears on the list of critical success factors of most major organizations. There are three fundamental qualities of information which are vulnerable to risk and which, therefore, need to be protected at all times, namely availability, integrity and confidentiality [6]. The risks that threaten the security of its information and computer resources need to be assessed and managed in proper way and the necessary security controls need to be implemented and managed effectively [1]. As the use of Information Technology has expanded, managers of organizations have come to realize that IT can be used to gain competitive advantage. The implementation of Information Technology involves significant risks both from external sources and from the technology and process of implementation. Information Technology Risk management is the art of recognizing the existence of threats, determining their consequences on resources, and applying modifying factors in a cost-effective manner to keep adverse consequences within bounds.

The risk connected with wide application of different information systems in business grows together with the increase of correlation from customers, business partners and outsourced operations. In not sufficient budgets on security the meaning of risk management grows, setting appropriate relations between level of threat and cost of appropriate protection [11].

Big enterprises are constantly under pressure of different kinds of audits indicating its efficiency in the scope of fulfillment of different requirements concerning information security. Management of risk in the enterprise requires more complex, mutual dependencies embracing business partners, services and outsourcing activity, and also consultants, partners and contractors. As it was mentioned many times, effective functioning of information systems depends on practices in the scope of security, and generally from management of IS security. One of the key processes in management of security is IT risk management, which is the process of achievement and maintenance of balance state between identified threats and activities undertaken in order to protect information resources [16]. The objective of IT risk management is to protect Information Technology assets such as data, hardware, software, personnel and facilities from all external (e.g. natural disasters) and internal (e.g. technical failures, unauthorized access) threats so that the costs of losses resulting from the realization of such threats are minimized. The purpose is to avoid or lessen losses by selecting and implementing the best combination of security measures [1].

Risk management involves the identification and implementation of effective security controls to mitigate, control and resolve the organization's risks [6]. Four major components of risk management, indicated in the literature, are:

- risk identification,
- risk analysis,
- risk-reducing measures,
- risk monitoring.

Risk management for IT begins with the risk identification process, which allows organizations to determine early the potential impact of the realization of internal and external threats on the entire IT environment [1]. Risk identification is the process of discovering, describing, documenting and communicating risks before they become problems and adversely affect the organization [15] [1] [6].

Next phase, IT risk analysis is undoubtedly key element of the process of Information Systems security management and therefore management of risk. Several methodologies are currently available to comprehend the extent of losses of IT assets from the realization of internal and external threats identified in the previous stage. These methodologies are categorized as quantitative methods (where estimation of risk value is connected with application of numerical measures), qualitative methods (these methods do not operate on numerical data, presenting results in the form of descriptions, recommendations, these approaches include scenario analysis, fuzzy metrics and survey questionnaires etc.) or hybrid methods, which are combination of both previous methods. Risk analysis is main process of risk management, which evaluates risks which have to be controlled, minimized or accepted. Correct assessment of risk and evaluation of its occurrence probability gives clear image of its impact on functionality of the whole Information System [1] [6].

Implementing measures to reduce IT risks is the third stage in IT risk management process. Necessary steps should be taken to ensure that the entire Information Technology environment is protected from all sources of identified threats. There are many various security measures that may be implemented to mitigate different types of IT risks. Three major types of controls can be implemented:

- Administrative controls (also called procedural controls) consist of approved written policies, procedures, guidelines and standards,
- Technical controls (also called logical controls) use software and data to monitor and control access to information and computing systems (e.g. passwords, data encryption, firewalls, IDS – intrusion detection systems, access control lists etc.),
- Physical controls monitor and control the environment of the work place and computing facilities and control access to such facilities (e.g. doors, locks, air conditioning, smoke and fire alarms, fire suppression systems, security guards, cable locks, etc.).

Last indicated phase is IT risk monitoring, which is an additional layer to safeguard the IT environment. Active risk monitoring ensures that effective counter-measures
to control risks are appropriately implemented and applied in the enterprise [1].

Information technology risk management embraces risks connected with application of Information Technologies in the enterprise i.e. protection of Information Technology resources, data recovery after failure or ensuring continuity of activity. For successful management of IT risk the people who manage enterprise must understand what is the attitude of enterprise towards risk, they should know regulations requirements, be aware of the main risks and theirs responsibility for the risk [12].

IT risk management processes should be aligned with legal and regulatory requirements and include or link to relevant activities such as privacy, information security assessments, continuity of business assessments, and business impact analysis. For large organizations to implement risk processes consistently, they must use strong communications, focused change-management processes, process guidance, and training [15]. Moreover, organizations undergo numerous regulations, concerning e.g. data storage, confidential information, financial responsibility and rules of continuity of management. Although that none of above requires elaboration of IT Governance structure, it may turn out that it is great way for ensuring compatibility with binding to company regulations.

By implementation of IT Governance there may be gained internal control, indispensable for meeting the most important of these regulations [8]. When implementing rules of IT Governance there should be done identification of the types of risk what will enable for definition of factors which can make difficult the realization of assumed business objectives. In the scope of this process one should concentrate on such aspects as [10]:

- Definition of tendency to risk and analysis of current events,
- Identification of the types of risk connected with information services,
- Definition of the types of risks connected with provision of new technological solutions,
- Correction of the scope of implementation on the basis of identified types of risk.

In design and implementation of IT risk management strategy in the enterprise there exist a need to integrate perceptivity of threats. There should be remembered that together with technology development and especially rapid growth of the Internet, and growth of information meaning for functionality of enterprises the threats in the business area and Information Technologies become more common and have different forms. Contemporary information systems created new types of risk and its security have global dimension with broader scope of Information Technologies. In such a situation, business risk is strictly connected with threats of information system security.

The aim of protections is minimizing risk of the loss of capability of operation. Management of IT risk embraces in its scope assessment of risk, setting priorities in the management of risk, implementation of means alleviating risk and consequent repetition of this cycle. Management of IT risk is a discipline integrating many different technologies used for identification, analysis, assessment for incidents and threats and also implementing means increasing security [11].

Management of risk is complex, interdisciplinary domain in the borderland of Information Technology, organization and law.

In the work [14, s. 289], taking into consideration classification of M. Porter, there were distinguished three fundamental variants of risk management strategy:

- **Strategy of concentration** (innovations) meaning implementation of modern protective solutions;
- **Strategy of diversification** meaning reliability, different systems and ways of protections;
- **Strategy of minimal costs** of protections meaning minimization of financial expenditures intended at security if IS.

The appropriate risk-managing strategy depends on the nature of the risk and other situational variables that influence the organization's range of choices. Strategy of risk management must evolve together with changing goals and business strategies of enterprise. It should demonstrate the following features:

- Flexibility towards increasing complexity and scale of threats connected with IS security,
- Emphasis the key meaning of people and processes,
- Evolution together with changing legislation, threats and control mechanisms,
- Enabling quick reaction on occurring threats and carriage of improvements.

Lack of appropriate management of Information Technology risk may have serious consequences for enterprise, because it can lead to the loss of customers, weakening market position, loss of prestige, disruption in cooperation with partners and contractors, and also it may generate significant costs. Important factor influencing increase of risk are the following changes: installation of new versions of applications, migrations of applications, updates, new hardware, new users and alterations in applications. According to research of IDC Company, one of the biggest companies dealing with research of telecommunication and Information Technology market, elaborating many sector analyses, over 80% of intervals critical for business in provision of services appears as a result of weak control over processes of changes [11].

There are many different IT risk management standards, methods and tools. ISO/IEC 27002 is probably the most widely accepted information security management standard including guidelines connected with risk management. Around 3,800 organizations have been certified against the certification standard ISO/IEC
27001. Other famous standard is recommended by NIST Special Publication 800-30 entitled “Risk Management Guide for Information Technology Systems” [16]. Australia/New Zealand standard AS/NZ 4360:2004 provides a generic guide to managing IT risk in a wide range of activities, decisions or operations. ENISA (The European Network and Information Security Agency) published a handy inventory of risk management methods and tools. There is famous risk management methodology, called CRAMM, formerly a UK Government risk management method, is now owned by Insight Consulting, part of Siemens. Other well-known methodology is FAIR (Factor Analysis of Information Risk), which is a method for analyzing information security risks, which recommends rigorous risk analysis process [2] [17].

Many large organizations build their own risk management systems or use multiple commercially available risk management software applications and packages [15].

4. PRACTICE OF IT RISK MANAGEMENT – SELECTED RESEARCH

As it was underlined, Information Technologies currently play tremendous role in functionality of enterprises. Automatically the risk connected with its work move directly onto business risk and business activity of the whole company. It is underlined many times relation, relying on appropriate matching of business and Information Technologies, being one of cardinal rules of IT Governance. However practice shows completely different situations, because conducted research commissioned by CA Company, conducted in Europe and Middle East by Freeform Dynamics Company among 715 managers of IT departments, conduct of consultations with managers and IT specialists is very often omitted in the process of planning business risk management. Moreover, in conducted researches 61% of respondents stated that risk is seriously taken into consideration in their companies but simultaneously higher level mangers of IT departments devote only 30% of their time to prevention of business risk [7].

In the research, over one third of respondents said that, in their organizations the risk is analyzed only in specified areas, and 4% of companies do not conduct such type of analysis. 80% of organizations claim that, anxiety of risk does not allow them fully to use contemporary technologies and modern practices, in such areas as automation of supply chain and advanced communication [7].

Many modern organizations created post of director dealing with risk (CRO). Task of this employee is to supervise risk management, especially in the case of financial services sector. CRO directors work in 48% of companies connected with financial operations (in comparison to 36% mean). However, one of the most obvious weaknesses is lack of arrangement of IT managers in defining requirements in the scope of risk management at business level. Taking into consideration dependency of effective risk management from possibilities and performance of IT systems, directors are advised to encourage and facilitate better participation in IT planning in the process of planning at the level of whole organization.

Organizations aspire to ensure greater coordination at the practical level between physical and information security of organization and between security and management of information. Organization’s expenditures on investments connected with information risk increases, however activities connected with its management are still fragmentary and are not cohesive. More than a half of organizations participating in research do not have separate budget intended at IT risk management nor at the business and information level.

Taking into consideration dependencies of companies from Information technology systems, organizations which seriously treat coherent management of business risk must make Information Technologies integral part of management process.

Results of research emphasized on the need of constant improvements in the management of information and its security in most of surveyed companies. 55% of respondents do not have general budget on management of risk for business or IT department, and only about 30% employ IT managers in discussions about business risk, despite that they think most of all about Information Technology risk [7].

Other researches were conducted by Ernst&Young Company in 2005 year. 33 enterprises took part in researches from Poland, representing different branches i.e.: banking and finance, insurance, telecommunication, oil and petrochemical industry and Informatics. Nearly 80% of respondents stated that in theirs enterprises exists formal function of information security management. However one forth of surveyed notice that information security function in theirs organization is not integrated with the process of risk management. These functions are realized separately, so undertaken decisions, unnecessary initiatives or such which focus on areas which do not contribute to improvement of general profile of organization’s risk. Many companies (38%) do not manage risk connected with subjects they cooperate with [7].

Only less than half of organizations take into account risk connected with the usage of new technological solutions. 16-30% of surveyed admit that they do not have any plans for the nearest year (if have such plans), which would took into consideration threats for information security. Furthermore, only 30% of organizations implemented system of risk assessment, of
which assessment of the risk of information loss is an element [7].

5. CONCLUSIONS

IT Governance is such an organization and realization of IT strategy of enterprise, which harmonize with business strategy, ensuring to the company achievement of its goals and introducing series of good practices and standards in the areas of Information Technologies. This concept includes such areas as strategic IT matching, provision of values by IT, effective use of IT resources, IT risk management and measurement of IT performance. IT security management and Information System risk management are crucial elements of discussed conception.

The risk, information security and the concept of IT Governance are strongly connected with each other and constitute correlative areas crucial for organization and application of modern Information Technologies in contemporary enterprises. Organizations are after all exposed on different types of threats, not only financial nature. Legislators, formulating legal regulations, taking special notice at operational threats, to which in a great extent belong threats connected with information infrastructure and Information Technology security. In the frames of correct management of Information Technology infrastructure there should be constantly traced threats, on which the enterprise is exposed and negative influence which they can exert on them. On this basis there should be made decisions concerning further actions, which can be concentrated on application of additional securing mechanisms, transferring risk onto partner or further risk monitoring [1][5].

Security of information and Information Technologies is a condition of its effective application in information-decisive processes of enterprises. Appropriate approach to the problems of information risk management, implementation of proper functions and protection and control mechanisms may decrease significantly probability of incidents avoidance, which could negatively influence on organization and also lead to lowering costs and contribute to gain of competitive advantage. However, as numerous researches show, in practice of different Polish enterprises approach to these problems is rather fragmentary and incomplete. Conducted currently in most of enterprises fragmentary and weakly organized activity in the scope of management and risk analysis does not guarantee appropriate effects.

6. REFERENCES