Enterprise Information Technology Security: Risk Management Perspective

Artur Rot

Abstract— **The risk connected with the wide application of information technologies in business grows together with the increase of enterprise's correlation from its customers, business partners and outsourced operations. Technological progress generates dependencies which evoke growth of diversities, complexity, non-descriptiveness and quantity of risk factors. In insufficient investments on information security the issue of IT risk management becomes more significant, concentrating on searching optimal proportion between threats and costs of IT systems protections. In such a dynamic development of Information Technologies the time needed for appropriate reaction on risk is decidedly shortened. The lack of appropriate preparation may lead the company to collapse, thus appropriate reaction on risk constitutes about possibilities of survival and development of enterprise. The problem of IT risk management is very complex issue. One of the most important stages of this process is risk analysis, used for optimization, and correctly for minimizations of losses connected with risk. The article presents the issue of IT security risk management, discusses the most significant stage of risk management which is IT security risk analysis. Chosen computer applications supporting these processes will be presented. Selected research connected with IT security risk management will be also discussed.**

Index Terms— **IT security risk, IT security risk management, computer support of risk management, risk management practice.**

I. Introduction To IT Risk Management

As enterprises 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 enterprises. 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 [5]. 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 enterprises 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.

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, 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 [13].

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 [5].

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 enterprises 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 [12] [1] [5].

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

Manuscript received July 26, 2009.

Dr. Artur Rot is with the Department of Management Information Systems Engineering, Business Informatics Institute, Wroclaw University of Economics, Wroclaw, Poland (e-mail: artur.rot@ue.wroc.pl).

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] [5].

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 [10].

IT risk management process 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 enterprises to implement risk processes consistently, they must use strong communications, focused change-management processes, process guidance, and training [12]. Moreover, organizations undergo numerous regulations, concerning e.g. data storage, confidential information, financial responsibility and rules of continuity of management [7].

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 [8]:

- 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 [9]. Management of risk is complex, interdisciplinary domain in the area of Information Technology, organization and law.

In the work [11, 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 [9].

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*” [13]. 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] [14].

Many large enterprises build their own risk management systems or use multiple commercially available risk management software applications and packages [12].

II. IT Risk Analysis as an Element of Risk Management

Analysis of IT risk is undoubtedly key element of the process of Information Systems security management and therefore management of risk. Publications connected with these problems – both domestic and international – seem to treat it in arbitrary way. It manifests in multitude of definitions of risk analysis, and also in the fact that risk analysis is often identified with its management [10]. Risk analysis is main and the most important process of risk management, identifies and evaluates risk which has to be controlled, minimized or accepted.

Risk analysis is comprehensive identification of threats and susceptibility if IT system’s assets and determination of the need of its control or acceptance of determined measures at previously stated level. The aim of risk analysis is provision of information which is indispensable for decision on application of specified methods, security resources in the enterprise.

Risk analysis inclines to carry out works in areas [3, p. 283-284]:

- Resource evaluation (information, software, hardware and physical resources) − value of resource it is not only value of its purchase but also short term effects and long term consequences from its destruction,
- Assessment of consequences − definition of the degree of destruction or losses, which can supposedly occur,
- Identification of threats − analysis of threats should determine probability of its occurrence and possibility of resource destruction,
- Analysis of protections in the aspect of effectiveness of existing means of protections,
- Analysis of susceptibility of particular IS resources,
- Assessment of probability, it is frequency of threat occurrence − this mark should embrace presence, duration time and strength of threat, and protections effectiveness as well.

Quantitative and qualitative methods are two fundamental groups of methods are applied for analysis of risk on which assets are exposed in enterprises. Groups of IT risk analysis methods [8]:

- Quantitative, where estimation of risk value is connected with application of numerical measures − value of resources is defined in amounts, the frequency of threat occurrence in the number of cases, and susceptibility by the value of probability of its loss, those methods present results in the shape of indicators. The examples of quantitative methods: Annual Loss Expected, Courtney’s and Fisher’s methods, ISRAM model, etc.
- Qualitative, which do not operate on numerical data, presenting results in the form of descriptions, recommendations, where risk assessment risk is connected with: qualitative description of assets’ value, determination of qualitative scales for the frequency of threat occurrence and susceptibility for a given threat or description of so called threat scenarios by prediction of the main risk factors. The examples of qualitative methods: FMEA/FMECA, The Microsoft Corporate Security Group Risk Management Framework, NIST SP 800-30, CRAMM.

Depending on the seriousness of a given threat there can be applied different risk measures from very simple assessments, determining the risk as high, medium and low, to very precise indicators presented as probability of a given event occurrence [9, p. 230]. In the case of evaluation of information security risk in Information System there is normally conducted qualitative analysis of risk. This method is most often based on information security criteria such as: confidentiality, integrity and accessibility. Full analysis of risk may be carried out separately for each of mentioned criterion. Correct assessment of risk and evaluation of its occurrence probability gives clear image of its impact on functionality of the whole Information System.

III. Selected Applications Supporting The Process of IT Security Risk Management

Management of Information Technology security especially in large enterprises is undoubtedly complex task, bringing many difficulties. In order to facilitate and increase effectiveness in this scope there were created many methodologies and standards supporting the process of analysis and management of IT risk. More than once on the basis of those standards and created on its fundamentals methodologies of risk analysis there were elaborated computer aided tools. The degree of complexity of contemporary Information Systems makes comprehensive and compatible with appropriate norms analysis of risk extremely difficult task for realization, especially without support of specialized software. Such a systems give more than once the possibility of automation of the risk analysis process in the Information Systems of enterprise and accessible presentation of its results for people responsible for security of information and for managerial staff of enterprise. They are mainly used for analysis and risk management and for current maintenance of defined level of security in organizations. Among such solutions there can be distinguished etc. [2, s.106]:

- questionnaires, forms, lists,
- office applications,
- simple tool applications,
- advanced, extended and comprehensive software used for analyses, tests in the area of system security,
- expert systems,
- specialized software for simulation and modeling.

As it was mentioned, those tools are more often implementations of selected standards and methodologies. Systems for the purpose of risk analysis are very significant group of IT tools which are used for analysis of dangerous hypothetical incidents and also systems of monitoring current events in the area of information security in enterprise, to which belong e.g. popular scanners and security testers [2, p.106].

As it was showed above, most of popular methodologies are computer supported and those applications were created on the basis of norms, standards or good practices. The examples of such systems are the following programs and IT packages: CRAMM, Marion, CORA, COBRA, MEHARI-Risk, RiskPAC or MAGERIT system.

CRAMM methodology accepted by CCTA (U.K. Government Central Computer and Telecommunications Agency), as governmental standard of analysis and risk management. The process of risk management according to this methodology consists of 3 subsequent stages [17, s. 44]: identification and evaluation of resources, evaluation of threats and susceptibility, selection and recommendation of control and protection mechanisms. Risk analysis of which the main aim is determination of probability of occurrence of incidents interfering correct functionality of resources, where identified resources are allotted to asset groups, for which there are generated lists of threats that could concern a given asset group, and there is determined level of risk for each group (in 5 degree scale). This methodology uses dedicated software, which is its integral element supporting listed particular stages.

The current version of CRAMM system is developed and offered by Insight. This is the package for analysis and risk management, which consists of 3 components, and is additionally supported by a large library of surveys, questionnaires and recommendations [16]. There are two basic versions of this system: simplified – "Express" and advanced to the professionals – "Expert" [2, p. 142-143].

CRAMM Express is the high level risk assessment tool that can undertake a basic level risk assessment for times when full risk assessments are not required.

CRAMM Version 5 Expert is positioned as the information security professional's tool for performing detailed risk analyses including those intended to support ISO 27001 compliance or certification programmes. Some of the main features included in the Expert version include [19]:

- the CRAMM Express function for initial high level risk assessments that is fully consistent with the existing CRAMM functions,
- the ability to expand a CRAMM Express assessment using CRAMM ' s other, globally proven, risk assessment functions,
- threat and countermeasure information relating to voice communications, wireless networking and penetration and vulnerability testing,
- expanded cross-referencing of CRAMM's countermeasures to ISO 27001's control objectives.

Version "Expert", which is essentially dedicated to the professionals, is enhanced in relation to the above version of "Express" and includes a risk analyzer, a tool supporting the implementation of the standard BS 7799, a library security, the wizard reports and a tool for helping drawing up contingency plans. Working with the "Expert" CRAMM system is connected with following processes and stages: preparation, analysis of resources, risk analysis, risk management [2, p. 143].

MARION is a package worked out in Great Britain by Coopers & Lybrand company and is used for risk analysis in commercial organizations. This package is based on library of currently known incidents; it includes many surveys and questionnaires applied for the evaluation of solutions in the scope of security. In case of risk analysis there was applied the method containing elements of qualitative and quantitative analysis. The software calculates results of analysis for 27categories of resources and threats. It allows for conduct of comparative analysis of results and creation of price data base for elements having influence on security. It allows for software evaluation of costs incurred due to improvement of protection system. Presentation of results is possible both in numerical and graphical forms. [2, p. 158] [16].

CORA system (Cost-of-Risk-Analysis System) is a system elaborated over 30 years ago by International Security Technology, Inc. The specialists dealing with risk define and store risk parameters in files as risk rules. These rules constitute later the basis of work for operational staff. CORA system provides the structure enabling storage of information. The estimation of potential loss is separately prepared for all elements of organization and the CORA is used for evaluation. Experts use CORA system for detection and storing data concerning susceptibility for all threats [16].

COBRA system (Consultative, Objective & Bifunctional Risk Analysis) is used for qualitative and quantitative analysis of risk and for assessment of compatibility of applied solutions with international standard in the scope of ISO/IEC 17996 information security management. The software is dedicated for experts in this field and its main element is set of automatically generated model forms and knowledge base. The basic modules of COBRA system are questionnaire creation module, risk/compatibility review module and reports from conducted analyses generator. This system consists of five basic tools [2, p. 151]:

- risk analysis tool (Risk Consultant),
- program for IT risk evaluation (PC Security Consultant),
- module for assessment of compatibility of applied solutions with British norm BS 7799 (BS 7799 Security Consultant),
- tool for analysis of compatibility of organization's functionality with accepted in it security policy (Policy Compliance Analyst),
- module supporting creation and evaluation of continuity plan (Continuity Consultant).

MEHARI it is methodology of risk analysis in Information Systems (Method for Harmonized Risk Analysis), and the program which was created on its basis MEHARI-Risk is a package of specialized software aimed at conduct of detailed analysis of IT system risk. MEHARI-Risk fulfils also many other functions supporting management of information security in the enterprise, including cost planning and ensuring compatibility with rules. The method of obtaining complete data about Information System which is indispensable for determination of risks for this system is internal audit what means examination of this system. Internal audit allows for definition of quality of protective services. Internal audit is indispensable for preparation of risk analysis and it is made by questionnaires containing questions for appropriate persons having contact with examined Information System [18]. MEHARI methodology implemented in MEHARI-Risk software allows for automation of the process of selecting questions for questionnaires. Thanks to appropriate and complete description of Information System, correlating functions and information of this system with resources and indication of threat scenarios and usage of appropriate correlation matrixes, selecting questions is in MEHARI methodology realized automatically. The system automatically generates audit questionnaires. After input of survey results to MEHARI-Risk, the system automatically defines risks for all selected for a given Information System scenarios of threats. The final result of system activity in the scope of information risk analysis is comprehensive report containing overall information [18].

RiskPAC package elaborated in USA by CSCI company (Computer Security Consultants Inc,) is prepared for conduct of risk analysis and definition of influence of this risk on business processes. There was applied in it quantitative and qualitative analysis of risk. RiskPAC software contains: tool for questionnaires design (Designer module), tool for management of risk review with the use of those questionnaires (Survey Manager).

The fundamental of program functioning is the process of responding to answers formulated in questionnaires, concerning enterprise and its Information Systems, networks, hardware, software, business processes, management. Received information may be presented in the form of reports, of which models are placed in reports library [16].

MAGERIT system (Methodology of Risk Analysis and Management of Information Systems of Public Administrations) is based on methodology recommended for institutions of public administration. It deals with three domains [2, p. 159]:

- description of methodology of analysis and risk management;
- preparation of possibly full information and grouping it in data base which constitutes initial product for appropriate assessment of risk;
- tool programming supporting implementation of method.

The advantages of mentioned above and also other IT systems of risk analysis process support are i.e. [16]:

- established ways of data input, easiness of access and usage of information saved in data base created for the purpose of carrying out analysis,
- possibility of data manipulation in order to depict influences and effects of different combinations of application of protections means and losses simulation,
- possibility of quick input of changes to diagnosed environment (assets and resources) and recognition of size of risk in institution.

IV. IT Security Risk Management in Practice

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. 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. In the research, over one third of respondents said that, in their enterprises 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 [6].

Many modern enterprises 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 enterprise.

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.

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 [6].

Other researches were conducted by Ernst&Young Company. 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 [6].

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 enterprises implemented system of risk assessment [6].

V. Conclusion

Taking into consideration dependencies of companies from Information Technology systems, enterprises which seriously treat coherent management of business risk must make Information Technologies integral part of management process. Security of information and Information Technologies is a condition of its effective application in information 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 enterprise and also lead to lowering costs and contribute to gain of competitive advantage. However, as different presented research show, in practice of different Polish enterprises approach to these problems is rather fragmentary and incomplete. In many enterprises fragmentary and weakly organized activity in area of management and risk analysis does not guarantee appropriate effects.

References

[1] K. Bandyopadhyay, P.P. Mykytyn, K. Mykytyn, *A framework for integrated risk management in information technology,* Journal: Management Decision 1999, Volume 37, Issue: 5, Page: 437 – 445

[2] A. Bialas *Information and services security in modern institution and company* (In Polish), WN-T Publishing House, Warsaw 2006

[3] N. Carr, *Does IT Matter? Information Technology and The Corrosion of Competitive Advantage,* Harvard Business School Press, Boston 2004

[4] A. Grzywak (ed.) *Security of IT systems* (In Polish), Jacek Skalmierski Publishing House, Gliwice 2000

[5] S. Halliday, K. Badenhorst, R. von Solms: *A business approach to effective information technology risk analysis and management,* Journal: Information Management & Computer Security, 1996, Volume: 4, Issue: 1, Page: 19 – 31

[6] K. Jakubik *IT creates risk in business* (In Polish), Computerworld, 14.02.2007

[7] R. Jesionek *Introduction to IT Governance* (In Polish), CEO – Top Managers magazine, 05.04.2008

[8] R. Kaczorek *IT Governance implementation guide,* (In Polish) CIO – IT Directors' Magazine, 05.04.2008

[9] J. Muszynski *Risk calculation*, (In Polish) NetWorld, 07.05.2007

[10] R. Orzechowski *Effective application of IT in the enterprise,* (In Polish) E-mentor no 3(20)/2007, June 2007

[11] M. Pankowska *Management of information resources,* (In Polish), Difin Publishing House, Warszawa 2002

[12] T. Purtell *New View on IT Risk: Building a successful Information Technology risk management program,* The RMA Journal. Philadelphia, March 2008

[13] G. Stoneburner, A. Goguen, A. Feringa *Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology*, National Institute of Standards and Technology, 2002

[14] K. Liderman *Risk analysis and information security in computer systems* (In Polish), PWN SA, Warsaw 2008.

[15] V. Tsoumas, T. Tryfonas *From risk analysis to effective security management: towards an automated approach,* Information Management & Computer Security Vol.12, Bradford 2004

[16] *Risk Analysis in Information Security Management,* http://www.wsbio.waw.pl/attachments/063_analiza_ryzyka_informacji.ppt

[17] M. Ryba *Multidimensional methodology of analysis and management of IT systems risk – MIR-2M* (In Polish), doctoral thesis, Cracow 2006

[18] *MEHARI-Risk – Multi-task System of Risk Analysis and Information Security Management* (In Polish), http://www.mehari-risk.pl

[19] *CRAMM.com – Risk Assessment Tool /The total information security toolkit*; http://www.cramm.com/