Risk Management in Informatization

Velibor Božić
General hospital "Dr. Tomislav Bardek"
Ž. Selingera bb, 48000 Koprivnica, Croatia
informatika@obkoprivnica.hr

Abstract. *Today we are faced also with the information deficit (not enough quality information that does not meet customer needs) and a surplus of information (the existence of quality information that is not sufficiently exploited by the user). Due to the existence of an information deficit and surplus we are often faced with dissatisfaction with the received information system. It is always left feeling that there is a large gap between investment and gain. Many studies (from Gartner onwards) indicate that a large percentage of information systems not being implemented in practice, and also a great percentage does not meet user needs. Because of the above facts, information technology is often not perceived as a serious factor in the business system. Moreover there is disappointment with benefits of information technology. The consequence is that the IT does not look serious, about IT bad decisions are made.. Such status of IT department is a major risk to the organization.*

The question is why the effects of informatizations are insufficient, why it causes customer dissatisfaction and results in poor decisions about information technology? What are the reasons for failure? The hypothesis which I shall endeavor to prove here is that the main reason for the above problem is inadequate risk management process in informatization (technological, organizational, financial and human risks). At the beginning, something about basics of risks (dictionary, types of risks, the current situation in the area, risk management results and at the end, the risk management model proposal that would allow reduction of the deficiencies found in the study.

Keywords. Risk, informatization, risk management

1 Glossary of Terms

Assets[2], [10] - all that has value to the organization

Information Assets –anything that has value to the organization in connection with the collection, processing, storage and transfer of information (software, hardware, netware, orgware, lifeware)

Control - allows you to manage risk, including policies, procedures, guidelines, practices or organizational structures. It can be administrative, technical, managerial or legal.

Guide - a description that clarifies what should be done and how to meet the objectives set out in policies.

Insurer of information processing - any system of processing information, services or infrastructure and the physical location at which the system is processing the information, services or infrastructure are located.

Information Security - confidentiality, integrity and availability of information; additional requirements are authentic, reliable and undamaged (accuracy).

Information Security Event – it is a phenomenon identified in the system, the state of the network or service that warns of possible violations of security policy, error control or previously unknown situation which may be security relevant.

The incident of information security - it is one or more unexpected information security events that have a significant probability of compromising business operations or pose a threat to information security.

The policy - overall intentions and direction, formally expressed by management.

Risk - a combination of probability of event and size effects (impact) event.

Risk Analysis - systematic use of information sources to identify risks and to assess the importance of risk

Assessment of risks. - the overall process of risk analysis and risk assessment.

Risk assessment –the process of comparing the estimated risk with respect to given criteria, with the aim of determining the importance of risk.

Risk Management – coordinated activities to direct and control the organization's risk, risk management typically includes risk assessment, attitude toward risk acceptance and risk communication about risks.

Relationship to Risk – the process of selection and implementation of measures to modify risk

The third party - a person or body independent of all stakeholders in the organization, doing something about items of interest.

Threat - a potential cause of adverse incidents, which can cause damage to the system or organization.

Vulnerability - a weakness of an asset or group of assets by one or more threats can exploit.

Results of achieved threats – Immediate negative consequences.

Impact of realized threats – indirect and long-term consequences of the obtained results on the efficiency and effectiveness of the organization.

2 Goal of risk management in informatization

Protect the confidentiality, availability and integrity of information. The elements that must be met for protection of information:

- Patients, the public, employees, laws and regulations, management, supervision (administrative council?)
- They must all be met in some way in the context of protecting the integrity, confidentiality and availability of information. When we protect dana, we must take into account the risks.

Risks:

- The confidentiality, integrity and availability of information affected by many threats that attempt to exploit the vulnerability. As a function of the probability of occurrence of threats that exploit vulnerabilities and the size effects that the threat could cause a risk occurs.
- . The protection of information systems with the risk must be reduced to acceptable levels.

The essence of protection management information systems (what is this about?)

Confidentiality, integrity and availability of information [7], [9] are exposed to risk. The increasing in risk threats, directly affect the system. Threats exploiting vulnerabilities of the system. The vulnerability of the system also increases the risk. The vulnerability of the system enables the exposure of assets (the information in this context). The property has a particular value system that affects the entire organization. The risk directly affects the value of the property by reducing it. Organizations (hospitals, in our case) has a specific security requirements. These safety requirements are met through specific controls. The controls are essential to reduce risk (satisfying the requirements for confidentiality, integrity and availability of information). Control helps protect against threats to the system. The protection system is closed with this.

Controls:

- Detecting - they reveal the attack on the system
- Prevention - protects the system from vulnerabilities, reduce incursions into the system and could be starters (drvers) for detecting controls
- Corrective controls - reducing incursions into the system as a result of vulnerability

3 Types of risk

3.1 Technological / Operational

- all risks [9], [10] related to hardware, software, network and perform daily tasks;
- unavailability of service risks (*infrastructure risks* - these risks are related to errors which are linked with system architecture,(the dependence of the proper performance of applications and IT services on hardware, network and operating system).The biggest risk here is linked with investment in infrastructure; *application risks* - insufficient application functionality, poor version control ... *data risks* - lack of good procedures to manipulate the data, low quality backup, the risk of data loss, the risks of ICT security - unauthorized access to data (lack of physical or logical protection of data and applications, unconcern about data integrity, availability to them, carelessness about accuracy and reliability of data, unauthorized access to the major servers and network equipment))

These risks are most numerous, but not so fatal to the functioning of the organization, although if they are long-term, they can affect on efficient functioning.

3.2 Financial

- Off informatization plan from financial plans
- Cost overruns
- Analysis of low quality or lack of business report analysis (because of forecasts for the project implementation costs or implementation of business processes)
- lack of scenarios development for maintaining business continuity in case of realization of a threat
- absent of insurace of the essential equipment

3.3 The organizational/strategic

- performance inability of key business processes, functions
- lack of resources for the process as the key link between them
- failure to identify key adverse events that affect the achievement of critical business objectives
- failure to recognize the capabilities and capacities that are essential for managing impacts that allow recovery of the organization at a satisfactory level of performance

These risks are closely associated with the implementation of business strategies. Detecting, analyzing and reducing these risks should be an integral part of the organization's strategic plan.

.

3.4 Human

Employees are a significant source of risks as well as the stability and success of the company. Because of these facts, the risks associated with employees are very important. These risks can occur intentionally or unintentionally. Some of them are:

- insufficient training of IT personnel and errors that follow because of that
- purposely causing errors and issues (" leakage" of confidential information)
- inability of key employees to perform their tasks (illness for example)
- dependence on only one employee (no replacement; knowledge is not structurally but intellectually)
- employees' strike ...

These risks can be overcome by constant training of employees, providing the conditions for satisfaction of employees (salaries, wages, good working atmosphere), recognition of non-worker, acquaintance of employees through constant communication with them, giving a personal example.

4 The process of risk management

The process of risk management [1], [2], [11], [13] is, in generally, the same in all approaches that can be found in the literature. The basic steps in the process of risk management are:

- Determination of context
- Risk estimate
    - o Identification
    - o Risk Analysis
    - o Risk assessment
- Responses to risk

These steps must be implemented at all levels of an organization. The only difference is whether the risks are considered at the strategic level, tactical or operational. At the strategic level, the bord discuss about risks, at the tactical level executives (heads, directors ...), and at the operational level about risks discuss the operational risk management (formen) and direct executors (the workers). All of them, in their segment must follow the above steps in the process of risk management. Here, very briefly about each of the steps.

Determination of context

Here, it is determinated the domain on which we focus in risk management.

Risk estimation

- **Identification of risk**

This is a crucial phase because it is needed to identify all threats to the system and every vulnerability which the threat could be used. Finally, as a result of pairs of threats and vulnerabilities and the likelihood it could be defined risk. Here is the problem of how to objectively identify threats and vulnerabilities.

- **Risk Analysis**

At this stage, the system analyzes identified risks, assess the likelihood of risks, their impact on performance. Based on the obtained results, the risk is assigned a certain importance.

- **Risk Assessment**

Ranked risks are assessed according to defined criteria. Criteria for evaluation should be defined in advance. They can be: the nature and type of effects that can occur and whether the measurable consequences, how is probability is defined, how long the effects will be exist, is the likelihood of occurrence reduce over time, method of determining the level of risk, the risk tolerance level, which level of risk requires a response to risk, which are the most important risks that require immediate action.

- **Responses to risk**

Here, it is defined response to risk in order to fix it, or reduced it to acceptable levels. Responses to risk can be: the avoidance of risk (not taking actions that could result in risk), risk acceptance (take action regardless of the risk), the destruction of sources of risk, transfer risk (switching the risk to another – e.g. insurance), the reduction likelihood of negative events.

In the risk management process in the informatization, the question is what kind of controls [1], [3], [4] in response to risk (at risk treatment) have to exist? What is necessary is: to include the duplication of resources, increasing the error tolerance level of the whole system, spare set of IT services (which would temporarily assumed the role of these that are at a standstill). It is important to make a plan of action in case of risk realization, it is necessary to set priorities (which the IT services necessary to deliver, and without which it might be). The plan is necessary to develop possible scenarios to achieve the risk, the scenarios should identify significant risks of IT services and act to them preventively.

5 Overview of the field

There are different approaches to risk management [1], [3], [4], [11]. Each of them have certain characteristics that highlights some of the attributes of risk. Here we do not intend to describe in detail each of the approaches but we stress two things:

- the advantages of each approach
- the lack of (disadvantages) of each approach

COBRA (C&A System Security Objective and Bi-functional Risk Analysis)

Advantages:

- flexibility (recognizes the new situation in the field of information technology, knowledge base is continuously supplemented)
- automatic adjustment - it is about how to respect the security requirements in each case with the assistance of questionnaires automatic generation based on information and knowledge base
- self-analysis - questionnaire module system is constantly checked with regard to the requirements which take place in the initial questionnaire
- testing solutions - there is the possibility of simulations the efficiency of individual control and simulation of the impact of threats to the controls; oon that way cost is reduced
- reporting - a reporting system that are not "designed"; they are a professional reports which are not intended for end users but for professionals who manage the risks

Disadvantages:

- requires a lot of expert knowledge, especially in the segment forming the base of knowledge

ISO 31000/31010

Advantages:

• it is an international standard that brings the principles and generic guide to implementation of risk management. It consists of: management principles, risk-controlled framework and processes for managing risks.

- it is clear, and ISO 31 010 provides an overview of techniques for the identification, analysis and response to risks
- emphasizes the responsibility of management for a successful risk management process

Disadvantages:

- tells you what to do, not how it should be done

GAO (General Accounting Office)

Advantages:

- it is formed on the basis of a series of case studies, developed from the practice
- emphasizes the importance of identifying threats and full involvement of government
- it is important to coordinate activities in risk management

Disadvantages:

- limited to certain areas, based on 30 case studies came to the risk management model that is limited to: multinational oil companies, regulatory agencies, financial institutions and IT companies

CRAMM (CCTA Risk Analysis and Management Method)

Advantages:

- requires the involvement of management
- emphasizes the quality of risk analysis and control (there are over 4000 risk controls)

Disadvantages

- the experience of people who implement CRAMM method is required

OCTAVE (Operationally Critical Threats, Assett and Vulnerability Estimation)

Advantage:

- participation of managers and IT professionals
- participation and cooperation of the administration
- Self-direction, adaptive measures, defined processes, foundations for continuous process, looking ahead, focusing on critical, integrated management, open communication, global perspectives, teamwork

Disadvantage:

- requires high-quality preparation workshop (expert knowledge); it is based on the knowledge of employees, rather than on measurements, formal proofs, etc.

NIST (National Institute of Standard and Technology)

Advantages:

- the possibility that after the system description, the activities taking place in parallel and that speed up the whole process
- defined phases of risk management that are intuitively clear and do not require extensive expert knowledge
- well-defined approach to implementation of controls

Disadvantages:

- not formally required the participation of board in the process, but it stands out the participation as a recommendation

MOF (Microsoft Operations Framework)

Advantages:

- based on the concept of ITIL v3
- there is a clear and consistent description of the risks (so-called statement of risk, there is defined a key reason for a service delay, the effect of delays, the list of threats that cause a delay and best practices to solve problems)
- intuitive and simple way of ranking the risks

Disadvantages:

- subjectivity in determining the criteria for the seriousness of the threat (low, moderate, high).
- possibility that risk analysis team is not competent enough

PMBOK (Project Management Body Of Knowledge)

Advantages:

- direction to aim, clear objectives, financial definition, definition of time
- existence of a plan to manage risks

Disadvantages:

- possibility of breaking the budget and time period of the project
- not precise enough in definition how to implement specific steps

THE RISK MANAGEMENT STANDARD

Advantages:

- risk management is defined as a central part of strategic management
- description of every risk is standardized
- risk management is a continuous process that is embedded in organizational strategy and embedded in implementation of strategy. It must be led by top management, but should not be defined only at the strategic level, but must be translated into tactical and operational objectives

Disadvantages:

1. Subjectivity in the assessment of:

o *The results of threats and opportunities*
o *The probabilities of occurrence of threats*
o *Probabilities of chance occurrence*

ISACA IT RISK FRAMEWORK

Advantages:

- the fact that the ISACA [15], [16] is an international organization with 86,000 members in over 160 countries and is the leading bringer of knowledge, certifications, community related with safety- information systems, corporate IT, with *IT risks* and compatibility with the legislation and regulations, is an advantage because it implies comprehensiveness of experiences and good practices in risk management
- it emphasizes the link risk management and business systems
- precisely defined roles in the processes (so-called matrix RACI)
- …

Disadvantages:

- demanding methods of risk management that requires precise adherence to the agreed activities if we wants to achieve success

COSO ERM APPROACH (Comitte of Sponsoring Organisation of the Treadway Comission Enterprise Risk Management)

Advantages:

- it emphasizes the role of management
- any uncertainty within the business system is defined as the risk
- it emphasizes the need for proactive action to manage risks
- gives the possibility that the risk is positive (that affects on value increasing)

Disadvantages:

- emphasis only on risk controls
- less attention is paid to identifying and analyzing risks

ISO27002:2007

This is the standard for establishing information security and risk management is an integral part of its.

Advantages:

- provides a context for risk management because the goal of information security is to ensure business continuity, minimize business risk, maximize return on investment and business opportunities.
- allows to reduce, primarily, operational and technological risks (physical, logical protection of equipment and the integrity, confidentiality and availability of information)
- well-defined criteria for a decision for risks acceptance or rejection

Disadvantages:

- does not say much about organizational risks

COBIT – Control Objective for Information and Related Technology)

COBIT [17] enables that managers, supervisors and IT users to have a set of measures, indicators, processes and examples (best practices) to help them to maximize the benefits of information technology and develop appropriate management and control of business processes in their organizations.

Advantages:

- four perspectives provides the ability to identify risks in all key processes of informatization
- ensures that risk management is fully embedded in management processes
- the possibility that the process of assessing and managing risk in the IT field ranked in different levels of maturity
- **…**

Disadvantages:

- COBIT is not an original method for managing risk and does not deal primarily with them, it primarily provides corporate IT (IT governance on all level of organization (corporation))

A variety techniques could be applied in each of these approaches, in different stages of risk management (risk identification, risk analysis and response to risks). The scope of this paper does not permit a description of these techniques and their specificity. Therefore, it is only listed here [12]: HACCP, ERA, SWIFT, the matrix of consequences / probabilities, RCM, HRA, decision tree, the analysis of causes and consequences, FMEA (FMECA), RCA, BIA, a method of scenarios, a preliminary risk analysis, loss of data analysis, analysis of financial reports, physical inspection, review of policies and procedures, controls, compliance with laws, flow charts, checklists and audit ...

6 Research

The survey was conducted between November 2011. year i and March 2012. year. It was conducted so that the e-mail questionnaire sent it to 22 government offices, 28 branches of county courts, 16 ministries (former government), 126 cities, 27 organizations and agencies, 43 health institutions (clinics, general hospitals, clinical centers, health centers) and 11 companies.. The questionnaire contained 41 questions and it was a semi-open type. Answers to some questions were offered (yes / no, grades 1-5), and on some issues was intentionally demanding more comprehensive response in order to gain insight into the experiences of others (and thus i was learnt).

Aim of research:

1. First : to prove that does not exist good risk management in informatization and that is one of the causes of customer dissatisfaction
2. Second: to see which areas are critical in the risk management (organization, technology, people or finance)

The questionnaire covered 34 processes in the field of information technology according to CobiT 4.1 and questions are formulated so, that questioned the existence of threats in each of these 34 areas. All questions are grouped into four domains, namely: planning and organization, acquisition and implementation, delivery and support, and monitoring and evaluation. Participants in the study were asked to respond to all questions and to answers both top managers and executives responsible for IT.

From sent 273 surveys, it was returned 116 which representing 42.49%. The response is an indicator of relationship towards risk management. From the surveys returned, two were almost empty, and all others could be used for analysis.

Results of research show that organizations in our country does not manage well with the risks (not involved in the identification of risk, don't management with them). IT is not seen as a relevant partner which is itself a risk to the organization. When we review the group of responses received in the survey, it is seen that result is a very unfavorable in the planning and organization, and monitoring and measurement. These are the areas of management responsibility, top management. Slightly better situation is in the procurement and implementation and delivery of support because this is the area of responsibility of executive managers. So the key risks because the informatization fails are organizational risks. The problems in the field of human resources, finance and technology arising from organizational risks.

Table below briefly mention the results of the survey - for each question, the greatest percentage of responses with a short comment.

			Summary of survey
Planning and organization	1.	What is the role of IT in decision making?	31% participate
	2.	Do you have information you get from the system of sufficient quality (reliable, comprehensive and accessible)?	58% yes
	3.	Do you use a standardized IT (comparable with the others)? Such IT better support process of decision making?	51% yes
	4.	What is the organizational position of IT in your organization?	48% deparment or lower
	5.	Is there exists cooperation between IT and other parts of the organization?	55% yes
	6.	Do you when investing in IT takes care of the financial viability?	72% yes
	7.	Does the financial plan for information technology an integral part of the financial plan of the entire organization?	62% yes
	8.	Does the board discusses IT? On the scale 1-5 rate the importance of information technology for administration (board).	38% 3, 4, 5 - important
	9.	Whether your organization is the learning?	41% yes
	10.	Are your employees computer literate? Znaju li se služiti aplikacijama, IT sustavom na zadovoljavajući način? They know ho	83% yes
	11.	Does IT products meet user needs (1-5)?	56% 3,4,5 -meet
	12.	Do you assess the risks of computerization?	45% yes
	13.	Do you managed with risks in informatization?	31% yes
	14.	Are you in control of IT projects?	62% yes
toring and evaluation	15.	Do you monitor the quality of IT services (applications)?	31% yes
	16.	Do you have defined parameters that are monitored for quality assessment of IT performance?	14% yes
	17.	Do you have control mechanisms that protect IT assets from destruction?	62% yes
	18.	Doyou take care that the IT services aligned with the laws, regulations and business policies (eg. licensing)?	29% yes
Acquisition and implementation	1.	Do you develop solutions alone or you have outsourcing?	69% outsourcing
	2.	Do you have have a maintenance agreement (SLA, etc.) with partners, where exactly is defined the obligations of partners?	76% There is agreement
	3.	Does outsourcing partner response to your requirements satisfactory?	69% yes
	4.	What is the response time?	52% now or till 24 hours
	5.	Do you have enough resources for the quality of IT service (for its continuity)?	58% yes we have
	6.	How many times in the past year the service was unavailable?	56% 2-4 times
	7.	How long (in time) IT service was unavailable?	61% up to two hours
	8.	Do the applications you used the right way?	79% yes
	9.	Do you have training of the user?	79% yes
	10.	Are you in control of IT costs? Whether they are seen as part of the costs of the organization?	74% yes
	11.	Do you have physical and logical protection (password) of IT services?	82% yes
Delivery and Support	12.	Is there a procedure for access to the server and the database?	62% yes
	13.	Do you have customer service?	79% yes
	14.	How you solve the incidents, errors that arise in dealing with applications (immediately react or waiting)?	71% immediately or almost immediately
	15.	Do you know at any time with anything available (The number of PCs, servers, routers, switches)?	90% yes
	16.	Is there a current listing of equipment?	79% yes
	17.	Are there records of the problems in using IT services?	66% yes
	18.	Do you take corrective and preventive actions regarding the problem?	65% yes
	19.	How quickly resolve user requirements?	68% immediately
	20.	Is there a procedure for data management?	55% yes
	21.	Is there a physical protection of IT resources?	72% yes
	22.	Is there a preventive maintenance and whether it planned?	62% yes
	23.	Do you monitor the performance of the IT services?	79% yes
	24.	Do you backup your data?	86% yes

7 New model of risk management in informatization

Informatization is a process of planning, analysis, design of ICT support, implementation and maintenance operations within the same organization. In this context will be examined and the risks associated with informatization. The study found that organizations which are surveyed in a small percentage identify risks (45%), much less manage them (31% manage). IT very weak standing within the organization (37% is considered IT important for business, in only 48% IT has been incorporated as part of the department or departments, in 69% IT in any way is involved in decision making, only in 38% cases IT is important for the administration in 55% of cases there is some form of computer communication with other parts of the organization ...). It was confirmed that IT is not accepted as a serious factor, which actually represents a risk for organizations that are nowadays more and more depend on IT and equipped with hardware, netwer, software without a clear vision of what to expect from ICT (ICT plans to advance only 38% of respondents, but at the same time, only 58% of them considered that the information is reliable, accurate, quality information; IT products meet the needs only 56% of users). Research has shown that the level of informatics (in the segment in which the CIO work) situation with risks are better, than the level of board (e.g. in 72% of cases there is customer support, in 82% of cases there is protection of information assets). There are problems with resources for quality IT service - in 58% of cases the resources are sufficient, the problem is licensing - 71% of respondents do not have all the software legally, 65% of responders taking corrective and preventive actions to solve problems; in 68% of cases it is tried to respond immediately when a problem occurs, 79% of respondents monitor the performance of IT services, in 86% of cases are being backed up, 62% of respondents indicated that there are preventative maintenance ... So, here I propose such a model of risk management in informatization that puts the emphasis on governance and management. The desire is to realize the best possible management of strategic risks and to emphasize the need for a comprehensive look at the problem.

On the other hand, based on theoretical considerations of the approach to risk management, I will endeavor to develop a model that would in some steps of risk management used the best from each approach. I will emphasize the techniques that should be used in each step.

Therefore, the proposed model of risk management in the informatization is the result of research about relation to the risks in organizations and reflections about the steps of risk management on the basis of existing approaches. MODEL (4x4 MIR-Management of informatization Risks):

It consists of four steps. These four steps are repeated cyclically at four levels (management, tactical management, operational management, employees) The model emphasizes the necessity of management (board) participation. The problem that we want to solve wit the new model:

The need to identify combinations of methods/ tools to meet the needs of the organization (for effective risk management).

Four groups were involved in the proposed model as follows:

- Top management
- Tactical (middle) management
- Operational management
- The direct executors - workers

All four groups of risk management go through four stages:

- definition of context
- identification of risk
- risk assessment
- attitude towards risk

Throughout all four phases is an important communication and control. ISO 31000 defines the identification of risk within the estimates (risk assesment). There estimate comprises: identifying, analyzing and evaluate risk. In this model, risk identification is extra stage because it is extremely important for further risk management process.

Identification

It begins with a checklist and review. They serve as a basis for further. When we have the basis of identified threats then we go on with: physical inspections, interviews with employees, examination policies and procedures, inspection of contract, loss of data analysis and final review of insurance policies. Finally, we have recognized the threat and we can go further in the process of managing them.

Prerequisites for the model:

• formed a team of people to implement the model
• defined objectives to be achieved in connection with the environment, operations and interdependencies in the organization
• detailed description of the activities and operations (resources, links, outsourcing partners interests ...)
• financial and operational consequences of loss within the critical process
• prepared questionnaires
• list of key employees that are thought to interview and list of shareholders, partners that are thought to communicate

Types of risks that are significant for this model:

Board

.*Risks on the corporate level.* They are risks in the IT areas that significantly affect the success of the business process. These risks are closely associated with the implementation of business strategies.

Detecting, analyzing and reducing these risks should be an integral part of the strategic plan of the organization. For these risks is responsible administration and executive directors of certain sectors

TACTICS

Risks of IT processes related to the core IT processes related to organizing and planning, procurement and implementation, delivery and support, and monitoring and evaluation within the information technology. These are the risks of conducting each of the 34 COBIT processes inside information, which helps managers to maximize the benefits of IT and develop appropriate management and control of business processes. The success of these IT processes responsible for the IT manager (CIO) and other executive directors, whose scope of work associated with informatization.

Operations

Operational risks are risks that arise in performing daily activities within a processes in the IT field. For them are responsible the immediate perpetrators of concrete activities (developers, designers, system administrators, database administrators, network administrators, and users of IT services. These risks have the most, but not so fatal to the functioning of the organization, although if they are long-term can affect the efficient functioning .

Each stage occurs at each of the 4 levels of the model only to a certain stage at a certain level using other methods / techniques (Figure 1).

	Context	Identification	Estimate		Treatment
			Analysis	Evaluation	
Board	SWOT	Matrix: Business Goals / Threats (Balanced Scorecard)	Matrix: Threat/4A; deciding what threats are primary or secondary for availibility, accurate, access and agility	Method SWIFT (Structured What-if Technique)-the size of the risk effects estimates and important risks are determinated	Determination of managerial control, particularly protection policy
Tactics	The scenario method	BIA method for each strategic threat	Matrix of „threat / likelihood of appereance“ and „realization of threats / impact on business operations“ for each threat which primarily affects on availability, access, accuracy or agility of IT	Matrix: „probabilities of threats“ / „impact of treats on business operations“ and ranking of risks for each risk who affects on system availability, accuracy of information, access to information and agility of system	Determination of menagerial controls - procedures on the basis of policy
Operat ional	FMCEA	Identification of threats with the help of a flowchart of the process	For each threat on the tactical level, which is defined as a critical: detailed development with techniques „cause / consequence“	Matrix:„probabilities of threats“ / „size of consequence“ on the higher degree of detail; Ranking of risks	Determination of operational controls in performing everyday tasks
Run of (perfor mance)	Working instructi ons	Threats detecting with method of causes and consequences	Observation method and errors / incidents notation	Ranking errors and incidents which are registrated. Criteria are: number of errors/ incidents, downtime and recovery time	Implementation of control mechanisms

Figure 1. 4X4 MIR model

8 Conclusion

Risk management generally, and so in informatization, represents a significant management skills for increasing safety and security within the organization (in ICT area too). Quality risk management enables that the results of informatization are acceptable to users and that management accepts IT as an importance partner for better and more efficient decision making. This text gives an overview of the field, it explaines risk management briefly, gives a briefly presentation of the research which has pointed to certain problems. At the end, I propose a model of risk management with which identified problems could be overcomed. The model should be confirmed in practice and this is the next step.

References

[1] Ž. Panian, M. Spremić et all.: “Korporativno upravljanje I revizija informacijskih sustava”, Zgombić & Partneri – nakladništvo i informatika d. o. o.”, Zagreb 2007.

[2] M. Crouhy, D. Galai, R. Mark: “The essentials of Risk Management”, The McGraw-Hill Company, New York, 2006.

[3] R. R. Moeller: “COSO Enterprise Risk Management”, John Willey & Sons Inc., New Jersey, 2007.

[4] C. Alberts, A.Dorofee: “Managing Information Security Risks: The OCTAVE Approach”, Addison-Wesley, New York 2009.

[5] P. Gregory: “IT Disaster Recovery Planning for Dummies”, Wiley Publishing Inc. New York 2008.

[6] S. Snedaker: “ Business Continuity & disaster Recovery for IT Professionals”, Syngress Publishing Inc., Burlington, MA, USA, 2007.

[7] G. Westermann, R. Hunter: “IT risk: turning business threats into competitive advantage”, Howard Business School Publishing, Boston 2007.

[8] C. L. Pritchard: “Risk Management: Concepts and Guidance”, ESI International Press, Arlington-Virginia, USA, 2001.

[9] J. P. Chavas: “Risk Analysis in thery and practice”, Elseiver Academic Press, London, UK, 2004.

[10] G. Monahan: “Enterprise Risk Management: A Methodology for Achieving Strategic Objectives”, John Wiley & Sons Inc. New Jersey, 2008.

[11] ISO/ IEC 31000:2008 Risk management – Principle and guidelines on implementation

[12] ISO/ IEC 31010:2009 Risk management – Risk assessment techniques

[13] HR EN ISO 27799:2008 Medicinska informatika – Upravljanje informacijskom sigurnošću u zdravstvenim ustanovama uz pomoć ISO/ IEC 27002 (ISO 27799:2008; EN ISO 27799:2008)

[14] ISO/ IEC 17799:2005 Information technology – security techniques-Code of practice for information security management

[15] “The RISK IT Practice”, ISACA Press, 2010

[16] “The Risk IT Practitioner Guide”, ISACA Press, 2010; “COBIT 4.1” ISACA Press, 2007.