INFORMATION SECURITY CRITERIA IN THE DESIGN OF BUSINESS SYSTEMS

Grzegorz Pieniążek, Piotr Zaskórski

Military University of Technology

Abstract. The paper presents the essence of the business system, its key features and capabilities of risk management. It identifies the design process of business systems and examines each phase. It shows the information security requirements for business systems and organizations.

1. Introduction

Business management is a process of harmonization of projects to achieve the objectives in an efficient and smooth manner (i.e. rationally using resources) and effective (i.e. leading to a desired result). The complexity of business management includes the size and diversity of the company tasks. The basis of the company's activities are repetitive actions (routine and statutory features) and unique action (ad hoc and current project), which are essential complements to repetitive activities. In the case of repetitive – especially those with high complexity – it is appropriate to pre-situational development of their implementation. This allows to determine the optimal mode of operation based on empiricism and analogy of behavior.

The project – according to the praxeological[1] definition – is a complex action, multi-stakeholder, carried out in accordance with the plan, which, due to complexity, requires selection of appropriate methods. The subjects of project management are complex tasks, referred to as projects. Each project defines a specific purpose. Project can be specified as "action taken to cause the results expected by the contracting authority"[2]. Another important feature of the projects is their uniqueness. Project "has usually the unique nature of both the concept and implementation"[3], and "is a response to a unit need"[4]. An important feature of the projects is their complexity, which can be specified as action covering "larger actions" "comprehensive", "multi-

1 T. Kotarbiński, *Sprawność i błąd*, PZWS Warsaw 1970, p. 193.

2 G.D. Oberlander, *Project Management for Engineering and Construction*, McGraw-Hill, Boston 2000, p. 4-5.

3 Strategor, *Zarządzanie firmą*, PWE, Warsaw 1995, p. 365.

4 Ibidem.

-subject", i.e. those "in which planning, directing and implementing the most part takes many divisions of a company[5] (or even many companies)". As an important feature of the projects shall also be their definite, i.e. "a clearly defined business"[6] and above all the implementation in a finite time interval with highlighted the beginning and the end.

2. The essence of the system and business process

Business system generally can be system working in many areas relating to:

- Research and growth, i.e. tasks leading to generate new products and modernize existing ones.
- Production, i.e. manufacturing processes leading to the manufacture of the product (e.g. computer disk).
- Marketing, i.e. activity related to sharing information about the product to the potential recipients (e.g. marketing) while collecting and storing information about the potential needs, which may directly affect the efficiency of research and design processes.
- Sales, i.e. processes linked with the supply of product to customers.
- Support/Service, i.e. processes related to efficiency and usefulness of product in the recipient.

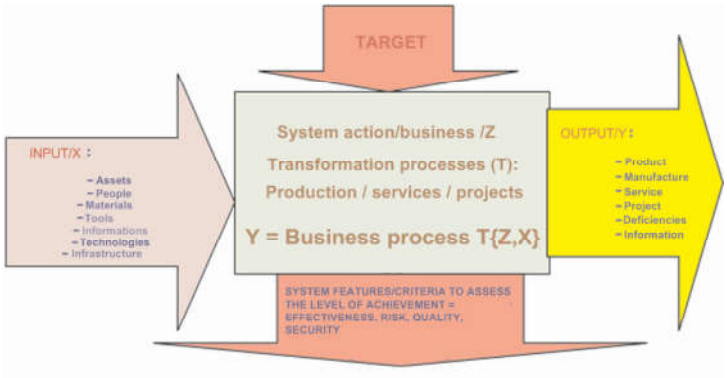

Fig. 1. Place of the business process (Source: own)

Each business entity can be considered as a designated areas system (fig. 1). This means that for his evaluation we can use the system criteria. One such criteria is the

[5] R. Hammer, *Technika planów sieciowych*, „Prace Naukowe Instytutu Organizacji i Zarządzania Politechniki Wrocławskiej" 1978, nb. 19, p. 81.

[6] B. Grupp, *EDV-Projekte in den Griff bekommen, Verlag für TÜV Rheinland*, Köln 1987, p. 7-8.

system security. Business system consists of a series of interrelated processes, defining the functional-task scope. The shape of the business system depends on industry, in which company functions. Business system should be:

- Logical, i.e. the reactions of the system should be forecastable/predictable by contractor/manager, as well as realization of task should cover sequence of logical steps, understandable for a man (potentially acceptable by the machine/computer).
- Consistent, that is, the individual components must cooperate with each other, so the producer did not have to learn each component from scratch, as well as specific action (e.g. action in case of error) should achieve the status of adequate standard.
- Complete, i.e. must provide all possible use cases, so it can't be that performer performing a task achieves a state of inability to perform (except, of course, incorrect operation/procedure).
- With reasonable complexity, i.e. should perform internally assigned to it operations, allowing the concentration on the most important aspects. Optionally, the company may operate on several business systems, and therefore there is an increasing emphasis on the integration of systems/applications supporting human activity. Also there are applications that are not relevant to the business, but only to support the work of other applications, as well as allow for automatic communication between those applications.
- Linked to a system for monitoring and managing risk. In the business systems we often deal with the concept of risk, which can be formally measured. When measuring risk we need to take into account several characteristics of those systems, such as:
- The availability, i.e. access to systems and data when it is necessary/justified. This allows you to assess the validity of specific data and systems for the organization function. Various data and systems in an organization require different levels of accessibility.
- Integrity, i.e. protecting against unauthorized modification of data, data protection against approved incorrect modification (to ensure that the data is processed in accordance with the objectives).
- Confidentiality, i.e. protection of information from unwanted disclosure (primarily intellectual property, personal data). This allows for regulatory compliance and privacy policy of organization.

In order to start risk analysis in business system, we must first identify the resources of the organization (property, assets), then assign the owners for those resources and to classify them to certain groups [14].

Every business organization is the executor of a set of processes [4]. Process must be seen as ordered sequence of changes in time and place and states occurring one by

one. The carrier of each process is always, in the result, a physical system. Each successive state/change of the system is caused by a condition/previous modification or by an external impact on the system [1]. The organization can distinguish processes:

- Basic, i.e. all kinds of system actions, such as the determination of organization policy and its quality objectives, continual improvement and upgrading processes and quality, system coordination (processes known as the main are associated with production of goods and services, supplies or design and control). This group also includes a degree of production, customer service, delivery of goods and carrying current and periodic control.
- Support, i.e. all tasks and activities related to general/basic security processes (checking and archiving a documentation, training or statistical service).

Process Management includes analysis, planning, organizing, monitoring, evaluation and standardization of isolated organization processes. The purpose of **process management** is to increase organizational efficiency by optimizing and standardization of processes [3] so that the same business activities generate certain specified costs, proceeded at a similar time and provide fixed quality of output. For process management there are tools used to manage knowledge about the processes and measure the effectiveness of processes. To standardize the processes there are used process management methodologies known colloquially as quality management systems.

Decisive factor about development of today organizations is the ability to use the intellectual potential of all participants in the organization supported by information technologies and automation [1]. As a result, it promotes the reduction of many levels of management. Created in the XIX and XX organizational structures and ways of working are no longer effective today. A radical response to the shortcomings of classical management business was Process Reengineering (BPR)7. Quality management is a kind of organizational culture – highlighting issues of quality and desire to achieve maximum success of the prospective client satisfaction, which is a philosophy of company and is not an action technique.

The concept of BPR process management is explained in many ways [1, 5, 14]. The most popular definitions are:

- analysis and design of activities and processes within and between enterprises,
- critical analysis and radical redesign of operating processes in order to achieve significant improvements in production rates,

7 This concept was first recognized and chosen to focus on managing the process and its analysis of the value and concept of value chain by M.E. Porter from the 80's.

– fundamental re-think of manufacturing solutions and radical redesign of processes in an enterprise in order to achieve substantial improvements in critical (evaluated) production indicators, such as cost, quality and productivity.

Process approach to management of the organization involves a thorough analysis of the processes at the interface between the organization and its environment as well as within the organization with particular emphasis on safety and continuity of its action [12]. Process management of the organization along with other management techniques such as management by objectives with the balanced scorecard, cost management and controlling using the method of activity based costing ABC (eng. Activity-Based Costing) is now the mainstream of changes in the management of modern businesses.

Process organization exposes transformation processes implemented by each business system. According to standard PN-EN ISO 9000:2000 process is a set of interrelated or interacting actions, which convert inputs into outputs[8]. Expanding the definition to business processes it can be said that the process is a set of activities or actions aimed at achieving the desired result and the process of fixing the value of the market position of a system-wide action. Based on the above definition, business process can be called a coherent set of sequence of actions aimed at fulfilling the expectations of the client, whose purpose is to achieve a specific value in the form of the product and the economic effect. Manufacture of the product must have the necessary resources, other products and a set of rules by which the product is created. State of the input process may be material or information, and the result is converted into a product that is subject, service or information. Resources necessary to implement the process are: equipment, methods, knowledge, skills, personnel and their qualifications. Product being at the output of the business process must be able to describe, to be measurable and unambiguous.

Way of modeling business processes results from the four basic levels of description of the organization. The highest level defines the company's strategy. At this level, actions are determined, the implementation of which will achieve the target of the business and ensuring business continuity. The level of business concept determines how the strategy will be implemented in the company, so the risk will become predictable. Implementing the business idea embedded in the organization determines what means (resources) will be carried out the tasks set out in the strategy and business concept of the separation of the so-called critical resources, determining its security and continuity. Only the lowest level specifies the implementation of the concept of business processes [4], whose security is a component of security throughout the organization. From this hierarchy results, that process-based approach is impossible to manage the company without the

[8] This definition is known as ICOM (called Input, Control, Output, Mechanism).

explicit determination of strategy and business concept and to establish measures and criteria for achieving the business target without identifying its component such as system risk and organizations security.

3. Information needs of organization

Information is one of the most important decision-making element in the organization. Lack of adequate information is the situation of uncertainty. This uncertainty may be due to lack of information or danger of acquiring uncertain information or distorted. Hence the desire to ensure that the increasing uncertainty runs safely processes of collecting and transformation of the information requested.

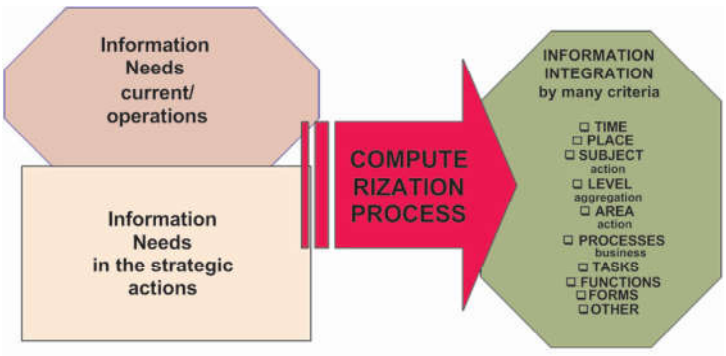

Fig. 2. The overall classification of the information needs of the organization (Source: own)

The amount of information is a multitude of data on the organization's activities, which are collected and interpreted by its members. Shaping the information needs is a long process, closely linked with the development and maturation of the organization. In the early stages a company usually focuses on the basic data and information necessary for market entry and survival. Only active participation in competitive markets enforce the collection and use of information dilated (fig. 2), which provide the potential for achieving competitive advantage. The scope of the operations of companies and their size or industry is also determined by information needs.

In large organizations operating in global markets, the complexity and extent of needs is disproportionately higher than in organizations focused on local market. This applies to both spheres of management and spheres of executive [10]. Changes in the business environment mean that the information needs arise and must be met using modern tools to improve business processes. These systems can eliminate the disadvantages of a strong hierarchical structures to flat structures/process, where the process becomes in fact the organizational object.

4. Design process structure

Any activity, including one whose subject is the realization of the projects, requires the creation of appropriate framework for action in a procedural (dynamic) and institutional (static) form. The basic, functional project management problem is to determine the structure of the project, i.e. consisting actions and their relationships. The main activity of the project is its execution, because of the vast majority of the time involved, human resources, material and financial resources and determines the outcome of the project. The design process includes activities and events that occur between the appearance of the problem and the creation of documentation that will describe the solution to the problem, satisfactory in terms of functional, economic and other requirements in the area of security solutions. Defining the project is implemented by the cells of the company competent to its analysis and evaluation. Phase of the project defining involves clarification of the project, analysis and risk assessment, estimation of costs and benefits associated with the project and taking the decisions by management of the project associated with designated project targets. One of the main objectives of the project is to ensure the security of the design and artifacts, which are the product of the project.

Project definition starts with clarification of the project. Clarification of the project requires the assembly of interdisciplinary knowledge. The essence of the project clarification is to draw up a comprehensive description of the key factors of the project. The scope should be tailored to the specifics of the project – its complexity, the degree of novelty – and the accepted rules of description. Base step is however, analysis and risk assessment of project (fig. 3). In theory and practice of management concept of risk is interpreted in different ways. Through the notion of risk is understood: first, the risk of losses, the possibility of injury or risk of economic failure; secondly, the possibility of negative variance between planned and realized result, and third, measurable uncertainty. Due to the complexity of the projects risk assessment is very difficult. It is necessary to carry out risk analysis, i.e. divide risk into its constituent parts and make their descriptions and estimate separately. The overall risk of the project consists of: market, organizational, technical, financial, personnel and information elements. In addition, the risk exists in various stages of the project and is associated with different sources – both with the environment of the project team and with its positions and organizational units. The risk of the project can be linked in varying degrees to individual elements of results of the project: requirements, costs and time and the scope of project. Results of analysis and risk assessment at the stage of defining the project are used to decide the appropriateness of the project. If you decide to implement a project, it is necessary to develop measures to reduce the risk (optimization/rationalization of the risk) and during the execution of the project controlling risk and taking appropriate countermeasures. For

projects with a high risk of quality to achieve the results can be used system of quality assurance similar to that used in manufacturing systems. This must be prepared in phase of preparing the project execution (planning project quality) and used in the execution phase of the project (study project quality and control of project quality). Conducted analysis provide the basis for evaluating the project, which is based on a comparison of expected benefits and the necessary expenditures for the project. In the case of projects we are dealing with complex benefits and expenditures, which include elements of both qualitative and quantitative elements (elements that are expressed with value and such, that cannot be adequately measurably). Based on the results of analysis and evaluation management makes a decision to proceed with the project. This decision must be confirmed after the completion of the development phase, in which will be concretized and detailed assessment of elements affecting the efficiency of the project and the expected level of quality of results, where exists the security component of the project and its results. Stage of defining the project ends with a determination of the objectives of the project, which concern, in accordance with previous considerations, three elements: the requirement for results/project scope, costs and duration of the project [8].

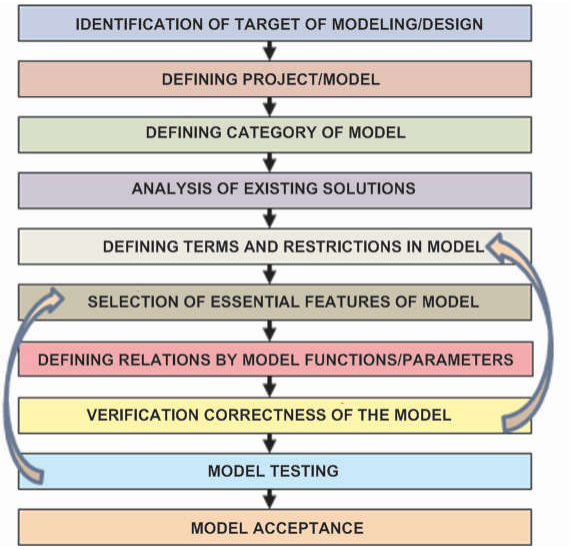

Fig. 3. Structure phase of the design/modeling (Source: own)

Modeling/design of business processes provides answers to questions about the activities of the organization and processes performed during these operations. Subsequently, it is possible to answer the question whether the processes are in line with company strategy and whether it is possible to improve the provision to

achieve a minimum level of risk [2]. The main benefits of the process modeling for each organization are:

- a single, structural description of the company, in which individual actors learn the principles of its functioning and its role,
- enable the precise mechanisms of tracking of implementation progress and the factors responsible for given stage of the process in system terms, i.e. the inter-relationships of organization potential with the achievement of maximum security for its operation,
- determine the optimal time, resources and costs of the functioning of the company, which factors determine the quality level and level of risk,
- standardize their operations and improve communication within the company and provide a basis for the implementation of quality management system (e.g. in accordance with the requirements of ISO 9001:2000),
- facilitate the selection and effective implementation of the integrated system supporting business management ERP (eng. Enterprise Resource Planning),
- identification and classification of areas for improvement, allowing for the improvement of the enterprise, and cleaning processes performed by the organization,
- improve ongoing processes in the dimensions of time and finance, as well as continuous monitoring of risk and results of the individual processes.

While improving the operation of the organization through business process modeling there can be distinguished business model, a map of business processes and maps of the flow of resources with particular emphasis on critical resources. The business model defines the organization's links with its environment and its interactions with the market environment. Diagram of the business model should include all key market players involved in the production of the company, as well as the flows of products and information. Map of business processes is a picture of all the functions necessary to produce the final product or products by the organization. Processes map should be possible to illustrate, using the symbolism of ICOM. Due to the uniqueness and obligatory of business processes at this stage are not yet modeled decision paths and critical conditions. The realization of the functions described by the processes determine the procedures and here is the place to modeling decision-making paths with a separation of threat, risk measurement and evaluation of resources security throughout the organization. In the ICOM definition a procedures are the control input for processes. Input of each process is inextricably linked to the scope of knowledge and information. Organization's information resources and their security are an integral part of the security of any business entity.

Good reflection of the various aspects of design and completely engaging structure of the design process of business systems is a UML[9], which is unified, standard language for modeling business systems including computer systems. Architect, designer or manager can use the UML diagrams in a similar way as a bricklayer or electrician use the architectural plan of the building.

Comprehensive and universal nature of UML, enables handling of object-oriented concepts such as objects, classes, attributes, relationships, aggregation, inheritance, methods, and others. UML is a set of concepts and graphic notations (diagrams), which allow you to comprehensively map the modeled area of the problem, the assumptions of the proposed system and the most important aspects of its construction. UML is now supported by many CASE tools. It was also accepted by the OMG standardization body[10] developing CORBA standard. It includes multiple perspectives of describing the system, which enables multidimensional analysis and the consequent quest for a full description of each process and its logical time compounds. This gives rise to the design of criterion of maintaining the security of the system and its resources. An important element is the concept of a class that allows you to connect processes with resources. In addition, it can be concluded that the use case diagrams and class diagrams, already provide a comprehensive picture of the behavior of the system. Other diagrams are important aids and can be used when creating the design documentation as required. Relationships between the different diagrams in UML are using the same names of classes and operations in different diagrams. Compliance of used names and their intuitive semantics are the basis for testing the mutual consistency of diagrams and their completeness and minimality, which promotes quality solutions.

5. Evaluation of risk in conditions of business informational asymmetry

Security throughout the organization and continuity of its functioning are strongly conditioned by the level of security of its information resources [2]. It is a category resulting from the essence of any system of action and assigned to its integral features. The security is inextricably linked to the risk, which may have a dimension of both positive and negative. In consideration of the organization security, it is appropriate to focus on the risks of adverse events and threats. Threats will usually reduce the value of each system. The organization is a system of action, which register the various threats to its operation. In the process organization – especially with security sensitive information resources – the problem of risk and

[9] UML – Unified Modeling Language.
[10] OMG – Object Modeling Group.

management of this area is a continuous process. Attempt to measure the level of the organization's security [11] leads to the observation that security is broad sense complement to the normalized level of risk:

$$B = 1 - Ry,$$

where: B – normalized level of security,

$$Ry = \mathrm{U}\,(\mathrm{P} \times \mathrm{W} \times \mathrm{D} \times \mathrm{E}),$$

where: U – normalization function of risk/normalized risk, expressed by point measurement,
P – level of incidence of risk,
S – level of loss,
D – susceptibility to vulnerability/resilience to threads/level of system security associated with the selected threat/risk source,
E – rate risk exposure.

Described above logical relationship means that the higher the level of risk is, the lower level of security may be. Risk management introduced a number of formal measures that allow quantification and validation of risk. Hence, there is also an attempt of formal valuation and assessment of security. This applies also the area of information security, which determines the security of processes and business organizations. Most of the information systems supporting the management of the organization has built-in security mechanisms, but not gives a full protection to information security. Each mechanism has determined level of security. To ensure continuity of information and decisions of the organization and internal and external security of the information resources, it is required a good choice in support systems. Integrated information management systems of OLTP class prevent loss, unwanted outflow[11] or distorted information. In decision support systems of OLAP class, mechanisms are fairly well complex and allow the selection of access to certain data groups[12].

Organization security involves also the positive aspect of informational asymmetry. This means that only certain information resources can be shared consciously to selected customers[13]. Certain stages of the selected process determines the extent of information made available to eligible organizations that participate in the wider project (process). But always there is the problem of security of information resources and their protection against unauthorized access, including the problem

[11] Including the encryption information mechanisms.

[12] This means that not all information resources of company can be made available in the environment further or closer. Value and security of organization is also measured by the level of security of its resources in the context of selective access of desired and undesired users.

[13] Mutual value of these resources in the process organizations doesn't have to be equivalent.

of continuity of action in various situations, particularly described as critical. Some of the information resources then receives the status of critical resources. Design of business organization is associated with the design of its critical resources, which includes information resources, data resources and software support systems, which operate in a networked environment, dispersed.

The design of each phase of this process is influenced by the quality of the project. Therefore, there must be the initiation phase, phase of identification and description of the current status, phase of analysis and optimization of processes with the phase of the development and verification of plan (fig. 3).

6. Requirements for the meta-model of organization information security

The knowledge and experience, and information resources and access to it, distinguish among entities of action (including designing entities) from each other and directly affect the effectiveness of the management process, from planning, through the organization of activities, supervision and coordination, and ending with the process control and evaluation. Hence, the security of information resources, particularly within the meaning of intentional access only to authorized entities is an integral part of security of modern organization, including security of projects and their results (fig. 4). Information and information resources – becoming a discriminant of the action subject for determining security in general – affect the ability to interact with the environment closer and further. There are problems of information asymmetry, which means that the various entities connected in a functional, process-oriented body can function properly if there is mutual trust, to the reliability and accuracy of shared information.

There are requirements for information security[14] (these are the basic requirements, which are universal and should be meet by the organization):

- Access Control, which means that organization must restrict access to the information system to authorized users under co-realized processes[15].
- Awareness and Training provides that managers and users of information systems are aware of security risks associated with their activities and the applicable laws, directives and rules, standards, instructions, regulations or procedures related to security of information systems[16].

[14] For example according to NIST (FIPS 200).

[15] Operated on behalf of authorized users or devices (including other systems) and the transactions and functions that authorized users can perform.

[16] This is to ensure that organizations personnel is adequately trained to perform their assigned duties and tasks related to information security.

- Control and responsibility are the statutory duty and organizations need to ensure business continuity: create, protect, manage and maintain documentation of an information system necessary to enable the monitoring, analysis, research and reporting of unlawful, unauthorized or improper system operations[17].
- Certification, accreditation and safety assessment is in itself a continuous process[18].
- Configuration management is associated with establishment and maintaining of output configuration of any system and the list of information systems[19].
- Emergency planning is associated with the establishment and maintaining crisis response plans[20].
- Identification and authentication are a form of securing users of information system[21].
- Response to event is a requirement for the security model in the scope to handle events in information systems that includes adequate preparation, detection, analysis, storage, recovery and response to adverse events.
- Service and maintain of systems supporting business processes in the periodic cycle and regularly perform conservation of information systems and provide effective control tools, techniques, machinery and personnel used to conduct information system maintenance.
- Physical and environmental protection is one of the most effective actions in the field of physical limiting access to information resources and equipment[22].

---

17 I.e. ensure that the actions of individual users of an information system can be clearly attributed to those users so can be adequate legal sanctions taken.

18 Organizations should periodically assess the security controls in information systems, develop and implement continuity action plans to correct deficiencies and reduce or eliminate the weak areas in information systems, to permit the operation of information systems and all communication with other information systems, control and monitor the security of information systems on an ongoing basis to ensure continued effectiveness and the degree of certainty.

19 Including the hardware, software and documentation throughout the life cycle and development of the system and to establish and apply the security settings for dedicated information products in information systems.

20 Backup and create disaster recovery plans for information systems to ensure availability of critical information resources and business continuity in emergency situations.

21 Processes acting on behalf of users or devices and ways to authenticate (or verify) the identity of the users (including the processes or devices) as a prerequisite for access to information systems.

22 Provide adequate working conditions for authorized individuals to protect the installations and infrastructure support systems, and provide tools to support information systems, protect information systems against the dangers of the environment, and ensure adequate monitoring of environmental protection in areas that contain elements of information systems.

- Planning already at the stage of design is an area conditioning good security check[23] in the storage place (or planned location) of information systems defined by rules of conduct in the case of individuals with access to information systems.
- Protection of workers provides that persons occupying positions in the organization (including service providers) are trustworthy and meet established security criteria for those items and, that organizational information and information systems are protected during and after personnel actions such as terminating or transferring.
- Risk assessment must be inextricably linked to the organizations security, which must periodically assess the risk to organizational operations (including mission, functions, or market position), assets and individuals, resulting from the operation of information and organization systems related to the processing, storage or transmission of information.
- Purchasing systems and services provides organization development and quality of business processes, which means that it is appropriate to release adequate measures to effectively arrange protection of information systems, to make appropriate life-cycle of processes which includes safety information[24].
- Protection of system and communication requires professional monitoring, control and protection of communication channels of key information systems, and introduces architectural models, techniques, software development and engineer systems, that promote effective information security policies in information systems[25].
- Integrity of processes and business systems and information resources (information), including support management systems becomes the challenge of time[26].

Developed and implemented model of the processes performed by the organization should therefore be able to be used when implementing a quality management system to meet the requirements of ISO9001: 2000[27] in:

[23] Document and periodically update and implement security plans for information systems.

[24] Limiting the use of software and ensure that cooperating companies use appropriate security measures to protect information, software and/or services.

[25] Including media protection, which is a requirement especially important for global/distributed/process organizations in terms of access to information only to authorized users and the physical removal/destruction of data.

[26] It is required to identify, report, and improve the information and eliminate the disadvantages of the information system in a timely manner, provide protection against malicious software features in the right places, and monitor reports of security information and take appropriate action.

[27] For example, in 4.1 of a point, saying among other things, that the organization should take certain actions.

- identify the processes, necessary for quality management system as a function of utility, efficiency and risk and their use in the organization,
- determine the sequence of these processes and their interactions,
- monitoring, analysis and evaluation of processes in terms of all system features including their security.

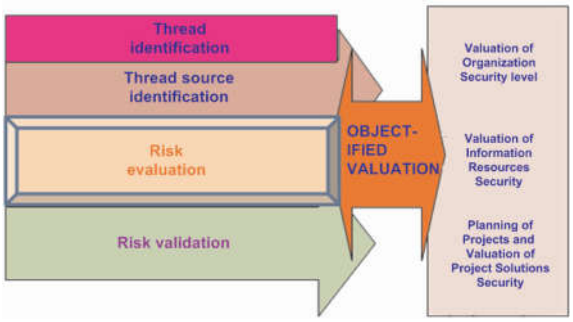

Fig. 4. A general model of the organization's security (Source: own)

Modeling and design of business processes is a major component of the design of business systems and information systems supporting in management of these processes. This also applies to corporate restructuring and diagnosis of adverse events in the functioning of the organization. A faulty or irrational process structures, more than other elements of the organization, may cause decrease in efficiency, safety and business performance. In some cases, only the understanding and improvement of implemented processes may lead to a general improvement in the condition of the company.

One of ways to use the business processes model is to support the implementation of a dedicated computer system. This support is particularly important when designing an information system based on SOA[28]. In addition, if the processes are modeled using the tools that have built-in mechanisms to exchange data with the tools of a CASE (UML) or ERP systems, it can be modeled using automatic processes to develop or implement an information system automating some processes. There is also a security criteria carried out within the meaning of the rendering of whole solution using generators producing software to support business processes in organizations.

7. Summary

Today's organizations are exposed to various threads associated with the creation and operation of systems supporting business activities, and in particular with information resources, which using these systems are stored, processed and transmitted.

[28] SOA – Open Systems Architecture.

This is due primarily to the loss, unauthorized reading and exponentiation of unwanted or lowering the desired – information asymmetry, which is important to maintain the continuity of the organization[29]. We must remember that information resources have often the status of strategic resources in building the value of each organization, serving the function of a critical resource.

Important is to introduce of appropriate measures at an early design phase (modeling). Risk management and other activities allow for the maintenance of information asymmetry on satisfactory level from the point of view of an organization, which will ensure its competitiveness in the market and an adequate level of information security. Very important is entire life cycle of the system and the design process, because allows to specify the requirements, the results of the project, project time and costs, including risk management and system security.

BIBLIOGRAPHY

1. J. Champy, *X-Engineering przedsiębiorstwa*, Placet Publishing Agency, Warsaw 2003.
2. FIPS 200 Minimum Security Requirements for Federal Information and Information Systems, 2006, http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf
3. B. Glinka, P. Hensel, *Projektowanie organizacji*, UW, Warsaw 2006.
4. P. Grajewski, *Organizacja procesowa*, PWE, Warsaw 2007.
5. T. Kasprzak (scientific editor), *Modele referencyjne w zarządzaniu procesami biznesu*, DIFIN, Warsaw 2005.
6. R.B. Kemball-Cook, *Luka organizacyjna*, Warsaw, PWE 1973.
7. G.D. Oberlander, *Project Management for Engineering and Construction*, McGraw-Hill, Boston 2000.
8. M. Trocki, B. Grucza, K. Ogonek, *Zarządzanie projektami*, PWE, Warsaw 2003.
9. J. Woźniak, P. Zaskórski, *Asymetria informacyjna w zarządzaniu bezpieczeństwem organizacji procesowych*, IOIZ Newsletter, Warsaw 2009.
10. A. Zając, *Wykorzystanie metafor do identyfikacji potrzeb informacyjnych*, „Zeszyty Naukowe AE", Cracow 2004.
11. P. Zaskórski, G. Pieniążek, *Ciągłość działania organizacji w warunkach asymetrii informacyjnej*, International Scientific Conference on "Zarządzanie kryzysowe – różne oblicza", Wroclaw 2010.
12. P. Zaskórski, J. Woźniak, *Ciągłość informacyjno-decyzyjna warunkiem bezpieczeństwa organizacji gospodarczej*, Conference on "Nowoczesne koncepcje i metody zarządzania – teoria i praktyka", WAT, Warsaw 2009.

[29] BS 25999-1: 2006: *Business continuity management. Code of practice.* BS 25999-2: 2007: *Specification for business continuity management.*

13. P. Zaskórski, *Zasoby informacyjne komponentem infrastruktury krytycznej organizacji*, V Międzynarodowa Konferencja Naukowa "Katastrofy Naturalne i Cywilizacyjne. Zagrożenia i wyzwania dla bezpieczeństwa", Wroclaw–Belchatow 3-5.06.2009.
14. P. Zaskórski, *Strategie informacyjne w zarządzaniu organizacjami gospodarczymi*, WAT, Warsaw 2005.

Streszczenie. W artykule przedstawiono istotę systemu biznesowego, jego najważniejsze cechy oraz możliwości zarządzania ryzykiem. Został zidentyfikowany proces projektowania systemów biznesowych oraz podział tego procesu na poszczególne fazy. Przedstawione zostały wymagania dotyczące bezpieczeństwa informacyjnego stawiane systemom biznesowym i organizacjom.