Risk management system as the basic paradigm of the information security management system in an organization

Romuald Hoffmann[1,a], Maciej Kiedrowicz[1] , Jerzy Stanik[1]

[1]*The Faculty of Cybernetics, Military University of Technology, 00-908 Warsaw, Kaliskiego 2, Poland*

Abstract. Risk is an inherent part of the functioning of every organization therefore the risk management should be a natural activity at each level of management. A common mistake in the management process of an organization is separating the security system, including the risk management system, and treating it as an isolated element. The article presents the place and role of the risk management system in the context of safety of the IT resource of an organization. A model of the risk management system was developed as the basic element of the organization management system and function supporting the continued operation in terms of IT safety of modern organizations.

Introduction

With the increase of changes in the surrounding environment, the management boards of various enterprises and organizations start to notice more risks of different type connected with business activities and start to pay more attention to the issue of security, including the information security. The issues related to the risk management system become an important element of the strategic management of enterprises and, in many cases, they are crucial for rationalizing the business activities and continued operations.

A common mistake in the management process of an organization is separating the security system, including the risk management system, and treating it as an isolated element. Our organizations already have different systems for process management, quality management, project management, objective management as well as control and internal audit, which on one hand are the perfect source of data for risk analysis, and on the other - provide knowledge of risks, vulnerability and potential of the said areas.

Many misunderstandings in the evaluation of the organization's safety often result from the lack of awareness and improper line of reasoning.

In the course of many disputes and proving one's reasons, the interlocutors often forget that the safety is not a state, but a constantly changing process, whose internal and external conditions to a different extent depend on an organization, to which they directly refer. Therefore, an important element in the process of ensuring internal and external security is the information security management system, which plays a key role in solving critical or crisis situations.

The knowledge of the level of the information security of particular business processes in the organization, including IT systems, allows to efficiently manage security by using dedicated risk management systems. To effectively manage the risk in the organization, it is crucial to be aware of the place and role of the risk management in the security management system.

The approach to the place and role of the risk management in the security system outlined in this study was presented in consideration of the fact that with the improvement of the functioning of the risk management system in the information security and the process undergoing therein, this place and role will be subject to change.

This document defined the essence of the risk, system components, model of the risk management process, role of the risk analysis team and approach to assessing the information security.

1 Organization as the system

The organization is a system aimed at achieving certain goals, whose subordinated parts/sub-systems co-contribute to the success of the entirety, and the success of the entirety is an important condition for success of every single part. The organization constitutes an internally integrated whole (system) composed of five basic parts (Fig. 1):

1. objectives and tasks – strategy system,
2. people (their efforts and patterns of behavior) - intellectual resources system,
3. material and technical equipment – technology system,
4. formal structure – structure system,
5. management element ensuring achievement of goals, survival and development of an organization in the conditions of the changing

[a] Corresponding author: maciej.kiedrowicz@wat.edu.pl

environment and requirements for the organization – management system.

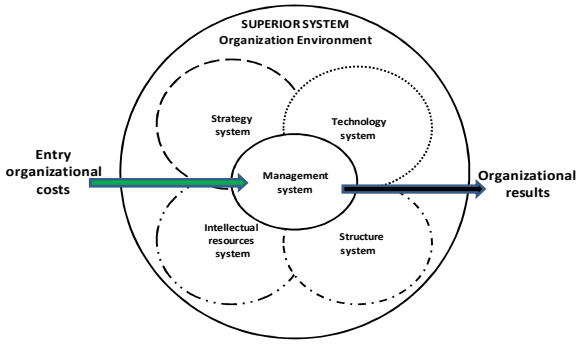

Figure 1 Model of organization in process terms

Environment of the organization - superior system composed of all external elements, directly or indirectly interacting therewith. The type of links between the organizations and the external elements allow differentiating the *closer environment* and *further environment*.

The management system is a set of operations:

1) performed within the area of the management function (planning, organizing, motivating, controlling) aimed at the resources of the organization (human, financial, material and informational), performed with the intention to achieve the objectives of the organization in an efficient and quick manner,
2) aimed at shaping fruitful cooperation inside the organization and matching these efforts with the requirements of its environment, in compliance with which the organization needs to function if it wants to survive.

The point of the management is to re-configure the functioning of the organization - using digital technology - in such a way that it is possible to use the full potential of the employees, business partners and clients to create and manufacture products and services with parameters satisfactory for the potential recipients in the second and next decades of the 21st century. The management changes the functioning of the organization in all its dimensions: from the organizational structures, communication, relationships with the personnel, through *information systems*, team work, arrangements with contractors, to relationships with the clients and public administration units.

For the purposes hereof, the organization is considered the system including the following sub-systems (Fig. 2):

1. The decision sub-system (control, regulation, management) - aimed at analyzing the conditions and inside of the organization, and making decisions with respect to the goals and missions as well as methods and programs of their implementation. It regulates the functioning of the organization by modifying appropriate stimuli compensating certain deviations (determined goals), which occurred during the operations of the system. It covers managerial position, hierarchical arrangements (organizational structure), and division of powers. The decision-making process requires from the decision-maker to define, analyze, assess and *take risk* as well as implement efficient measures. Due to its specificity, the system is closely related to the informational system. It is impossible to manage any organization (enterprise) with the information flow.
2. The information sub-system - an essential component of the efficient functioning of the organization, since - as mentioned above - the exchangeof information is a prerequisite for proper cooperation. The role of the informational system is to satisfy the informational needs of the decision-makers, since to make the right decision, they need to be provided with the necessary data. The informational system integrates technology with human actions in the organization. It covers all elements related to the exchange of information, i.e.: sources of origin of the information, its flow and manner of transfer, points of its collection and transformation processes. The informational management system is a set of operations and measures for collecting, finding, storing, sending and processing the information in such a manner so that it is possible to make decisions and manage an enterprise on the basis thereof.

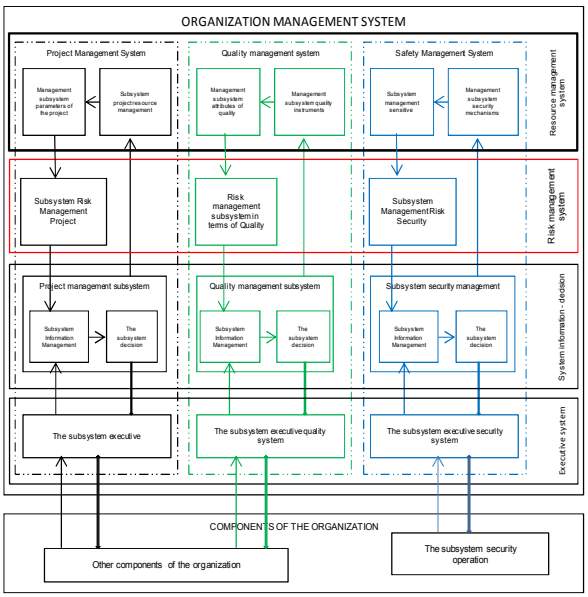

Figure 2 Sub-systems of the organization management system

3. Executive sub-system, which implements the tasks determined by the management arrangements. Its aim is to process the materials, raw materials and other resources during the technological processing. It includes direct production units, executive units, support services and other entities having direct impact on the transformation (processing) of resources and performance of services.
4. Risk management sub-system/system.

The levels of area-oriented security of the components of the organization determine the security level of the functioning of the organization. The functioning of every

component (area-oriented) of the organization may be disrupted by the following:

- natural threats: floods, weather conditions, windstorms, etc.;
- technical failures of the devices and systems, e.g. interruption of power supply, IT breakdown, etc.;
- hazards of civilization: chemical, radiation, communication, etc.;
- threats results from the location and regional specificity, among other things, e.g. smuggling, ethnic and/or religious conditions, etc.;
- destructive human activity.

The particular types of risks may occur at the same time and negatively impact the components of the organization. Furthermore, they might interact synergistically, which should not be omitted in the analysis of comprehensive safety of the organization. The security of the functioning of the organization is ensured by:

- continuous prevention of occurrence of particular types of threats to the functioning of the components of the organization (facilities);
- proper preparation of the facilities and services responsible for the area-oriented protection of the organization against any potential types of risks;
- undertaking of efficient remedial actions in case of their occurrence;
- restoration of the functionality of the facilities affected by some risks after their elimination.

The security level of the organization, within the comprehensive meaning, depends on the area-oriented levels of security. A specific, area-oriented level of security of the organization may be obtained in a number of ways - not only by ensuring certain efficiency of the security system directly preventing some of the occurring events. Its value may be affected by the following:

- prevention of the occurrence of a given type of risks;
- preparation of an entity for the potential activation of a given risk;
- security in the form of an event (education, location and availability of prevention measures);
- increase in efficiency of the security measures and mechanisms, while combating the effects of a given event;
- efficiency of actions aimed at removing the effects of a given event.

Therefore, we have a possibility of shaping the area-oriented and comprehensive level of security. In this case, the controllable values are the parameters characterizing the factors affecting the security level of the organization, i.e. connected with the following:

- prevention of any potential threats to safety of the organization;
- preparation of the organization in case these threats activate;
- security mechanism combating such threats;
- removal of the effects of a given event.

2 Model of the security management system of the organization

Many misunderstandings in the evaluation of the organization's safety often result from the lack of awareness and improper line of reasoning.

In the course of many disputes and proving one's reasons, the interlocutors often forget that the safety is not a state, but a constantly changing process, whose internal and external conditions to a different (sometimes large) extent depend on an organization, to which they directly refer. Therefore, an important element in the process of ensuring internal and external security is the information security management system, which plays a key role in solving critical or crisis situations.

The security management system of the organization is a part of the entire management system, based on an approach as resulting from the business risk, referring to the establishment, implementation, use, monitoring, maintenance and improvement of the security of the organization (Fig. 3).

It is assumed that the objective of the security management sub-system of the organization is to maintain the required security level of the organization as the functional entirety and to ensure security of the sensitive materials. This objective may be achieved by current control of the executive sub-system of security measures. The security management sub-system of the organization is composed of the following sub-systems (Fig. 3):

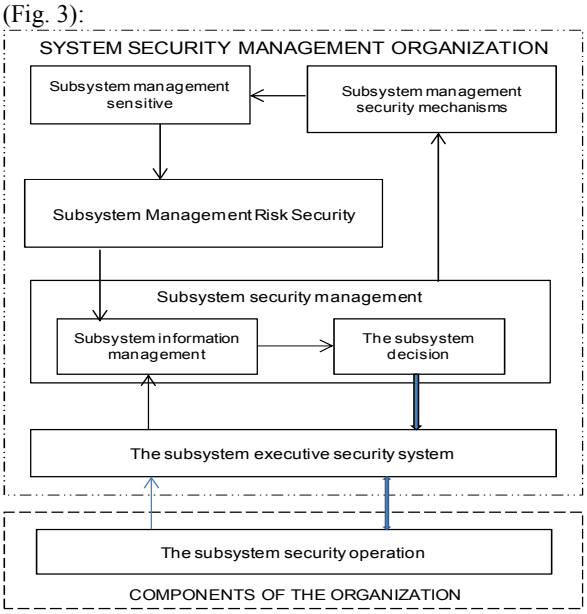

Figure 3 Functional structure of the security system

[*Organization Security Management System*]

- the security management sub-system, which implements the information and decision process, determining the manner of ensuring safety of the individual facilities in the organization by means of the executive sub-system,
- the executive sub-system, which consists of various measures for implementing executive processes,
- the security management sub-system,
- the management sub-system of sensitive materials,
- the risk management sub-system,
- the technical system supporting the management system and other components of the organization,

- the IT systems supporting the management system and other components of the organization.

The security management process in the organization should be performed in a continuous manner, constantly improved and implemented according to the plan, including the determination of the risk level, i.e. the tolerance threshold that - in case of exceeding - will make it necessary to manage this risk.

3 Model of risk management

A common mistake in the management process of an organization is separating the risk management system/process and treating it as an isolated element. Our organizations already have different systems for process management, quality management, project management, objective management as well as control and internal audit, which on hand are the perfect source of data for risk analysis, and on the other - provide knowledge of risks, vulnerability and potential of the said areas.

For the purposes hereof, the following definition of the risk management system of the organization was adopted:
"The risk management system of the organization is a set of rules, mechanisms and tools (including i.a. the policies and procedures concerning risk identification, measurement, monitoring and control) used for risk review processes in the organization".

The main task of the risk management system in the organization is risk identification, measurement or assessment and monitoring of the risk in a business activity of the organization, aimed at ensuring correctness of the process of rending office services.

3.1 Objectives, tasks, elements of the risk management system

The objective of the risk management system is permanent risk reduction, protection of sensitive resources, systems and processes, as well as protection against any potential effects of such risks. The risk management system should allow retrospective evaluation of the efficiency of actions undertaken with respect to:

- business process of the organization,
- employees and users in the organization,
- appropriate technologies.

The main tasks of the system include:

- provision of the information about risks and their profiles;
- performance of preventive actions reducing the risk and its consequences;
- monitoring of the acceptable risk level.

The elements of the operational risk management system of the organization are the following:

- strategy and policy rules of the organization with respect to risk management;
- by-laws and procedures defining the risk management process;
- the risk management structure defining the management levels as well as the scope of competency and responsibility of the persons involved in the risk management process;
- employees involved in the risk management process (their credentials);
- IT support of the process;
- management information;
- system control.

The strategy, including the policy contained therein, determines the objectives, basic rules and a set of guidelines concerning risk management. It provides grounds for developing detailed regulations and procedures.

3.2 Model of the risk management process concerning security of the organization

"Risk management" means the planned application of the management policy, procedures and practices as part of the activities concerning the risk analysis, valuation and control (Fig. 4). The risk management process supports and improves the operational efficiency of the management of the organization, as it helps to understand and assess serious risk factors. Therefore, the point of the risk management in the organization should be:

- obtaining the information about potential risks and their impact on the future form of the outside environment of the entity;
- defining the effects of the current events, which may have some impact on the functioning and the results of the organization;
- developing appropriate operational procedures (preparation for the consequences) for emergency situations, in particular for unpredictable risks.

The risk management process is a continuous process, which should be in the form of an ordered sequence of subsequent events, actions, decisions, resulting in a positive value, i.e. the security of the entity. Therefore, identification of a potential risk (crisis) is the key task aimed at avoiding surprise, such as, for example, a crisis situation. We should be aware of the fact that to efficiently deal with the risk analysis, it is crucial to define this risk as precisely as possible, by determining its causes, scope, limits and type of potential threats that may affect the achievement of the objectives stipulated by the entity.

We should realize that the risk analysis is a fundamental element of the risk management system in the organization, since during the risk analysis process, we obtain the information indispensable to make right decisions concerning the strategy of handling the risk, efficient choice of the risk reduction measures, assessment of the transfer validity, acceptance or avoidance of the rusk. From the perspective of the organization management, this important information, obtained in the course of the risk analysis, also indicates the priorities for the development of the security systems, security measures and control in the organization. Therefore, the statement that the risk analysis is used for the purpose of the mitigation (optimization) of the losses

connected with the operational risk seems justified. At this point, we may ask the question why there is more and more emphasis on the risk management. The answer is pretty simple - the "real life" examples show that in case of uncertainty and a possibility of risk optimization by removing often unnecessary, inefficient, yet expensive protection measures - such approach seems to be reasonable. The traditional protection of all activity areas of the organization seems to be excessively costly and inefficient, as usually there are not enough resources (cost-effective variants). Therefore, it is necessary to not only avoid and reduce the risk, but also to efficiently manage the risk.

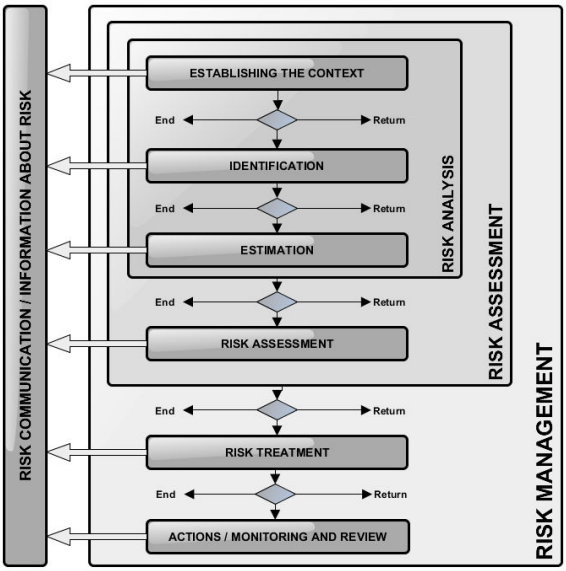

Figure 4 Model of the risk management process in the organization.

As shown in Fig. 4, the risk management process referring to the security of the organization may be iterative. The iterative approach to the risk assessment process may be in the form of increasing the level of detail of each iteration or stopping the process - after each phase/stage, there are decision points (continue, end, return).

The iterative approach ensures beneficial balance between the reduction of time and efforts spent on identifying some security measures and the certainty of the correct assessment of large risks. First, we need to set the context. Then, the risk assessment is performed. If as a result of the risk assessment, the sufficient information is obtained to determine the actions necessary for the purpose of modifying the risk to the acceptable level, then the task is considered completed and the risk handling process may commence. If the information is insufficient, the risk assessment iteration is performed once again in the changed context (e.g. risk assessment criteria, risk acceptance criteria or effect criteria), if possible, in the limited part of the entire scope. The risk acceptance should ensure that the residual risks are deliberately accepted by the management of the organization. It is especially important in the event when the security measures are not implemented or their implementation is postponed, e.g. due to costs. The efficiency of the risk handling process depends on the results of the risk assessment. It is possible that handling the risk will not lead directly to the acceptable level of the residual risk. In such case, if necessary, the next iteration of the risk assessment with the changed context parameters (e.g. risk assessment criteria, risk acceptance criteria or effect criteria) may be required, and only after this iteration, the risk is processed again.

Conclusions

Nowadays, the risk management processes with respect to the security of information should be an integral part of daily operations of every organization. To make these processes efficient, it is crucial to determine which management actions, method, techniques or tools will be the best for the organization. To efficiently implement the risk management policy in the organization, it is important to first define the objective and tasks of these units within the scope of risk management and make them compatible with the general strategy of the organization. Since the risk is an inherent part of the functioning of every organization, the risk management should be a natural activity at each level of management. It is a common opinion that the risk is always managed, but not always intentionally.

The process or processes of the risk management system constitute an element of the decision-making process, which make it easier for the managerial staff to make intentional and right decisions, determine the priority actions and recognize alternative ways of actions in case of present threats, events or critical situations.

Thanks to the risk management system, it is possible to improve the integrated security and quality management system, show the directions of the necessary changes that need to be introduced in the environment, indicate some priority actions and potential losses, if such event occurred. Such analysis enables to take preventive measures, which lead to the mitigation of the losses.

The risk analysis and assessment is the first element in the risk management process. The results of such process help to choose the appropriate systems or security methods as well as to minimize or eliminate the identified risk factors.

The risk management policy to a large extent depends on the nature of the business activity, its approach and tendency to take risks, also known as the "appetite" for risk, and business environment conditions. To support the process of introducing and maintaining the efficient risk management, it is indispensable to reach "common understanding" of the risk management system within the entire organizational unit and its environment. Without a common ground for discussion on the risk management system in the business operations of the organization, it is not possible to ensure powerful communication and introduce efficient risk management process within the entire organizational unit. It is impossible to manage something that is not explicitly defined and identified or understood in the same way by all employees of the organization. The risk management system is perceived in a different manner by the employees working on

different levels of the organizational structure (higher management, medium management, average workers), responsible for particular business process (main, auxiliary processes) or located in different organization units (headquarter, branches) of the same organization. The practical solution to find the "common understanding" of the risk management system in the entire organization is to apply the standard valuation model and risk assessment model.

References

1. M. Bielski, *Podstawy teorii organizacji i zarządzania* (C.H. Beck, 2002)
2. A. Białas, *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie* (WNT, 2007)
3. K. Jajuga, *Zarządzanie ryzykiem* (PWN, 2009)
4. A. Korczowski, *Zarządzanie ryzykiem w projektach informatycznych. Teoria i praktyka* (Helion, 2013)
5. P. Matkowski, *Zarządzanie ryzykiem operacyjnym* (Wolters Kluwer Polska, 2006)
6. J. Monkiewicz, L. Gąsiorkiewicz, *Zarządzanie ryzykiem działalności organizacji* (Uczelnie Techniczne, 2010)
7. O. Patrick, *ISO 31000:2009 Risk management – Principles and guidelines*
8. J. Stanik, M. Kiedrowicz, *Selected aspects of risk management in respect of security of the document lifecycle management system with multiple levels of sensitivity*, Information Management in Practice, 231-251 (2015)
9. *PN ISO/IEC 27001 Information security management. Requirements*
10. *PN ISO/IEC 27005 Information technology. Security techniques. Information security risk management*
11. *PN-ISO 31000 Zarządzanie ryzykiem – Principles and guidelines*
12. *PKN–ISO GUIDE 73 Risk management – Vocabulary*