Method for assessing efficiency of the information security management system

Maciej Kiedrowicz[1,*], and *Jerzy* Stanik[1]

[1]Military University of Technology, Faculty of Cybernetics, Urbanowicza Str. 2, Warsaw, Poland

Abstract. The article addresses the issue of efficiency assessment of the security system (SS) in terms of the Information Security Management System (information resources of the information system in an organization). It is assumed that the purpose of such security system is to achieve a declared level of protection of the information system resources. Therefore, the level of security of information system in a given organization shall be determined by the efficiency assessment of the security system. The efficiency of the security system mainly depends on the functional properties of its components and other factors occurring in its environment. The article mainly focuses on security configuration, i.e. technical configuration and security organization configuration. The thesis was adopted that the efficiency of the security system may be considered as a set-theoretic efficiency sum of the security configurations invoked in such system. Additionally, it was assumed that a prerequisite for the desired measures (indicators) of the efficiency assessment of the SS shall be to propose such measures and develop appropriate ways (methods) of their calculation. The efficiency measure for the SS as well as two methods of efficiency assessment of the SS were proposed in the article.
Key words: security, security system, security configuration, configuration of security measures, loss of efficiency of the security system.

Introduction

Based on the specialist literature, no methods of efficiency assessment in terms of the Information Security Management System were found. The lack of appropriate methods or criteria makes it difficult to perform quantitative efficiency assessment of the security system and requires the application of the qualitative assessment method. The qualitative assessment is subjective and its results, i.e. acceptance of the protection level of the resources or their rejection, depend on the knowledge and experience of the assessor. Efficient protection of the information resources in the organization requires implementation of various types of security configurations, including application of several or a dozen or so technical and organizational security measures at the same time. When we consider a group of such security measures and different characteristics of their correlations (relationships, properties), we are dealing with the security system.

When designing, choosing and assessing efficiency of the security measures, it is important to consider the following three complementary points of view:

1. how to mitigate the risk of losing security attributes of the protected resources (risk orientation or security attributes),
2. how to eliminate or reduce the risk of particular resources (risk orientation),
3. what can be done to protect the resources against the risks or vulnerability (resource orientation).

However, no security measures should be implemented if the risk level is tolerable, even in case of vulnerability, as the risks that may use such vulnerability remain unknown. All of the above-mentioned limitations determine the choice of specific security measures [1-5].

The article concentrates on efficiency assessment in the Information Security Management System. It is aimed at showing the whole spectrum of theoretical concepts, practical methods and approaches to efficiency assessment of the security system.

1. Place and role of the security system in the security environment of the organization

The security system constitutes a component of the Information Security Management System in the organization and is used for the protection of both the information systems and infrastructure as well as the information against any deliberate or accidental damage. Figure 1 shows schematic representation of the organization from the point of view of controlling current functionalities of the information system and maintaining the required level of the information security.

* Corresponding author: maciej.kiedrowicz@wat.edu.pl

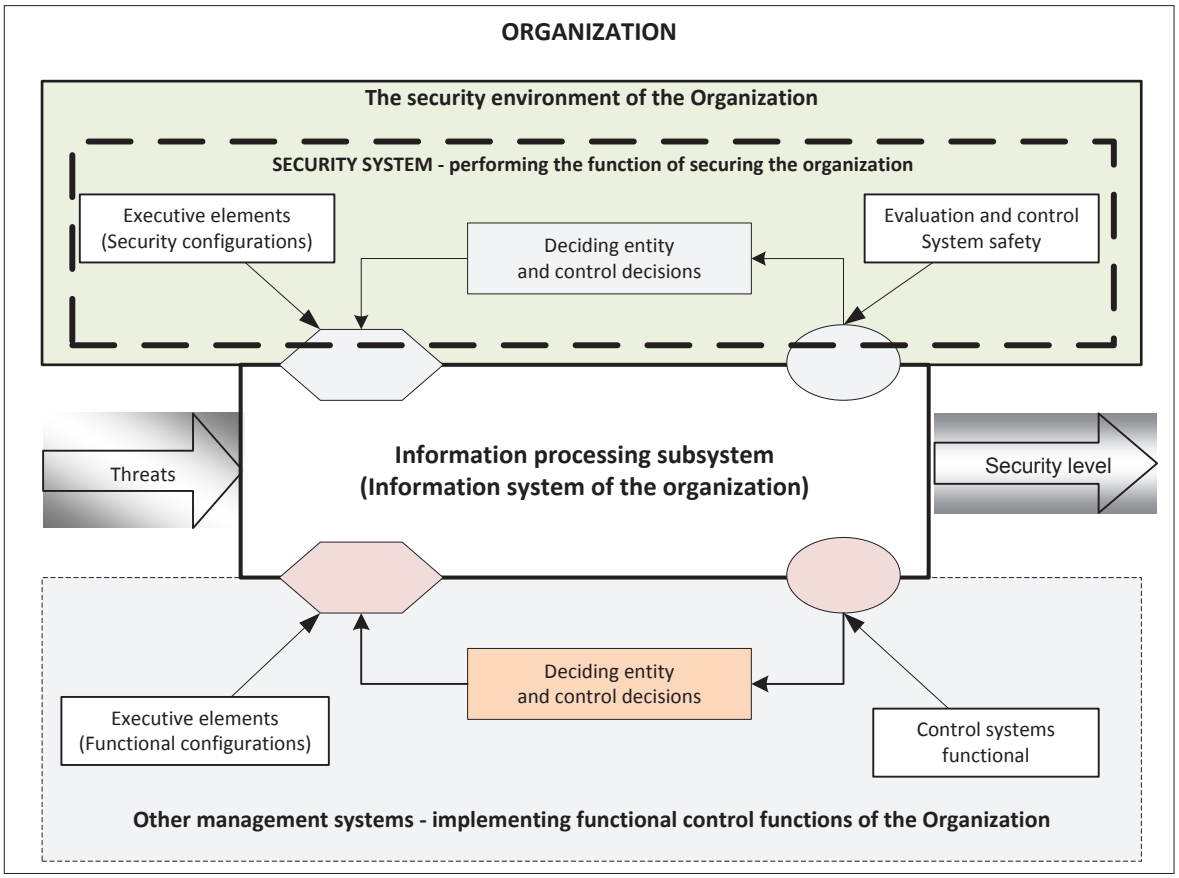

Fig. 1 Diagram of the organization from the point of view of controlling current functionalities of the information system.

Three elements are distinguished in the figure:

- Subsystem for information processing (Information System of the Organization),
- Security environment of the organization, in which the functions for controlling the security level of information resources are implemented.
- Other management systems used to implement the functional properties of the information subsystem in the organization.

Generally, in the descriptive sense, it is assumed that a given security system operates efficiently if the objective is achieved - the planned tasks are completed. Nonetheless, to reliably assess: the desired scope of the preventive and preparatory measures as well as forces and means necessary to efficiently react to certain risks, i.e. efficiently ensure an agglomeration of a desired domain-specific security level of its functioning - it is necessary to adopt a specific measure (indicator) of efficiency. It allows to assess and analyze the cost and possibilities of adopting certain solutions (concepts) for the purpose of agglomeration (in particular, its components) of the desired security level of the operations.

2. Measure of efficiency of the operations of the Security System

The security level of the information resources in the organization is the outcome of efficiency of the operations of the currently implemented security configurations in the security system. Two types of the security configurations may be distinguished in the security system:

- configuration of technical security measures,
- configuration of organizational security measures.

The configuration of organizational security measures is reflected by managing and administrative aspects of the information security, including liability in terms of risk management. The configuration of technical security measures is reflected by technical aspects, mainly relating to security groups: security of equipment, management of systems and networks, controlled access to the network, controlled access to operating systems, controlled access to applications and information, mobile processing and remote work, correct application processing, cryptographic security measures and security of system files. It is a good practice to use different security combinations, both organizational and technical.

The security combination may fulfill a number of functions, e.g. reduction, prevention, dissuasion, detection, monitoring, raising awareness, reconstruction, improvement.

The purpose of the SS is to allow certain information resources realize their tasks in the event when their functioning is disrupted by risks and vulnerability. The degree of implementation of a given task by the SS depends on the degree of implementation of the tasks by its security configurations, i.e. SCs. Therefore, the level of efficiency of the security system is determined by the level of efficiency of its security configurations.

The degree of completion of the task (guaranteed safety of the operations of the information system in the company) by the SS and SCs shall be called efficiency of the SS and efficiency of SCs, respectively. Therefore, the efficiency of the SS and efficiency of SCs shall be deemed to mean compliance of the obtained results with the intended operations of a given security system of the organization.

Generally, in the descriptive sense, it is assumed that a given system operates efficiently if the objective is achieved - the planned tasks are completed. Nonetheless, to reliably assess: the desired scope of the security mechanisms necessary to efficiently react to certain risks or vulnerability, i.e. efficiently ensure the security level of the information resources - it is necessary to adopt a specific measure (indicator) of efficiency for each security configuration. It allows to evaluate and analyze the efficiency of the security system as well as the level of security of the information system in the organization.

The following characteristics of the efficiency measures are provided in theoretical studies relating to efficiency assessment:

- compliance with the intended operations of the system,
- compliance with the efficiency indicator of the operations of the master system,
- sensitivity to changes in the values characterizing material utility properties of the system and its components,
- possibility of setting the values,
- possibility of interpreting the changes in the values.

The essence of the proposed approach to the quantitative efficiency analysis of the security system is presented below. The symbols are the following:
W - efficiency measure of the security system,
Ω - a set of possible measure of the W values,
I- a set of numbers of the SS configurations, $I = \{i: i = 1, I\}$,
J- a set of numbers of the security functions of the SS, $J = \{i: i = 1, J\}$.
W_I - the value characterizing efficiency of the i-th configuration, w_i - implementation of the value W_I, whereas $w_i \in W$,

W_{Ij} - the value characterizing efficiency of the i-th configuration with j-th security functions, w_{ij} - implementation of the value W_{Ij}, whereas $w_{ij} \in W$.

"Participation" in the efficiency of the i-th configuration with j-th security functions and protection against different types of risks shall be defined on the basis of the following correlations:

$$W_{Ij} = W - W_{\bar{ij}} \text{ or } W_{Ij} = \frac{W - W_{\bar{ij}}}{W} \quad (1)$$

whereas $W_{\bar{ij}}$ - efficiency of the security system without the i-th configuration with the j-th security functions. It is stressed that with the adopted manner of evaluation of the "participation" of the i-th configuration with the j-th security functions, the following correlations occur:

$$W_i \neq \sum_{j \in J} W_{ij}; \quad W \neq \sum_{i \in I} W_i \quad (2)$$

The above results from a possible synergy of effects of the interaction of the organizational and technical security configurations as well as from different functions used therein. Therefore, the efficiency of particular security configurations in terms of ensuring security of the information system of the organization shall be defined through the impact of their participation in the subject undertaking as regards efficiency of such system and the security system.

The above-mentioned approach to the efficiency assessment of the security system or its components (security configuration) allows to determine usefulness (role and weight) of both the security system and its security mechanism configurations in terms of ensuring safety of the information resources of the information system in the organization.

The efficiency of the security system depends on the following factors:

- a number of the protected information resources of the information system,
- a number of risks and vulnerability characteristic of the information resources,
- quantitative and qualitative selection of technical and/or organization configurations,
- efficiency of particular security configurations,
- a method for managing various configurations of the security mechanisms,
- an approach to efficiency assessment (applied method of efficiency assessment).

The model efficiency measures of the security system may be, for example, the following:

- a degree (indicator) of compliance of the applied security mechanisms (measures) in the aforesaid configurations of the security system with the list of security measures specified in the standards, e.g. compliance with PN-ISO/IEC 27001:2014-12 [6] or PN-ISO/IEC 27002:2014-12,
- a value of the reduced risk $\Delta R = R_p - R_k$, where R_p – value of the initial risk, R_k – value of the final risk; risk after applying security mechanisms
- an indicator achievement of acceptable risk level

– other methods.

In connection with the ever-changing external conditions of the organization, it is necessary to modify the implemented security measures, which makes it indispensable to undertake the following actions [7]:
– monitor and assess efficiency of the security measures, both organizational and technical;
– identify risk and develop rules of risk management;
– implement modified security measures;
– develop current declaration of use of security measures.

The recommended standards, including PN-ISO/IEC 27001:2014-12 or PN-ISO/IEC 27002:2014-12, do not specify which method should be used for the best results, therefore, the companies may apply their own methods, developed on the basis of the industry-specific knowledge and experience. Such approach is appropriate for large corporations, which have proper organizational structures allowing developing and validating such method.

3. Method for assessing efficiency of the security system aimed at compliance with the standards

Due to a variety of the resources, risks and issues related to their protection, the organizations create special policies, also including the information system security policy or plan. [8] describes present implementation the security policy, it is essential to choose appropriate security measures. It is a complex process, which should include the following aspects: technologies, procedures, human resources and physical protection. It is important to understand how each of these measures impacts the organization. It may be useful to consider the instructions included in the following norms: PN-ISO/IEC 27001:2014-12 or PN-ISO/IEC 27006:2014-12 [9]. The ISO/IEC 27001 standard (Appendix A) outlines 114 security measures[1]. The ISO/IEC 27006 standard (Appendix D) divides security measures into organizational (113) and technical (40) security measures. 39 security measures are classified both as organization and technical[2].

The method consists in the development of a declaration of suitability for use of the security measures, based on the security specifications included in the ISO/IEC 27006 standard (Appendix D)[3], and its comparison with the specifications of the implemented security measures.

The knowledge of security declarations makes it possible to determine a set of permissible security configurations (both technical and organizational) with appropriate features, having established a set of information resources, set of security attributes and set of risks and vulnerability connected with such information resources.

Therefore, let use introduce the following notation of any security configuration:

$$KZ_{klmn} = \langle A^{klmn}, AT^{k}, ZG^{l}, ZP^{m}, MB^{n} \rangle \quad (3)$$

where:
– A^{klmn} – a set of information resources of the information system in the organization subject to protection by the klmn-th security configuration,
– AT^{k} – a set of security attributes assigned to the information resources belonging to A^{klmn},
– ZP^{m} – a set of vulnerability describing weak points of the information resources from A^{klmn},
– ZG^{l} – a set of risks that may use the vulnerability of the information resources from A^{klmn},
– MB^{n} – a set of security mechanisms creating the klmn-th security configuration.
– The knowledge of the meaning of the security configuration allows to indicate a set of permissible configurations:
– on the basis of the set of the security measures included in the declaration of suitability for use (DSU):

$$KZ_{dop}^{DSZ} = \begin{cases} \{KZ_{klmn} = \langle A^{klmn}, AT^{k}, ZG^{l}, ZP^{m}, MB^{n} \rangle \in Å \times B \times \Omega \times \Pi \times \Psi^{DSZ} : \\ A^{klmn} \supset A_p\}, if \ \bigvee_{\langle k,l,m,n \rangle \in K^{v} \times L^{s} \times M^{r} \times N^{u}} (A^{klmn} \supseteq A^{p}). \\ \Phi \ in \ other \ cases - set \ empty. \end{cases} \quad (4)$$

– on the basis of the set of the security measures implemented under the security system (SS):

$$KZ_{dop}^{SZ} = \begin{cases} \{KZ_{klmn} = \langle A^{klmn}, AT^{k}, ZG^{l}, ZP^{m}, MB^{n} \rangle \in Å \times B \times \Omega \times \Pi \times \Psi^{SZ} : \\ A^{klmn} \supset A_p\}, if \ \bigvee_{\langle k,l,m,n \rangle \in K^{v} \times L^{s} \times M^{r} \times N^{u}} (A^{klmn} \supseteq A^{p}). \\ \Phi \ in \ other \ cases - set \ empty. \end{cases} \quad (5)$$

where:
– Å – a family of sets of information resources, which may have to be protected in case of lost efficiency of the SS,
– *B – a family of sets of security attributes, which may be assigned to information resources,*

[1] ISO/IEC 27001:2013 Information technology – Security techniques – Information Security Management Systems – Requirements. ISO, Geneva 2013, p. 10-22.
[2] ISO/IEC 27006:2015 Information technology – Security techniques – Requirements for bodies providing audit and certification of the Information Security Management Systems. ISO, Geneva 2013, p. 29-34.
[3] SSD - a document, in which the purpose of using the security measures as well as the security measures relating or applicable to the Information Security Management System in a given organization are described.

- *Ω – a family of sets of risks, in case of which the security mechanisms must be applied,*
- *Π – a family of sets of vulnerability of information resources,*
- *Ψ^{DSZ} – a family of sets of security mechanisms, which may be built on the set of security measures included in the declaration of suitability for use (DSU),*
- *Ψ^{SZ} – a family of sets of security mechanisms, which may be built on the set of the security measures in good working condition included in the security system (SS),*
- *A^p – a set of potential information resources,*
- *K^v – a set of indices of the family elements B,*
- *L^s – a set of indices of the family elements Ω,*
- *M^r – a set of indices of the family elements Π,*
- *N^u – a set of indices of the family elements Ψ,*
- *The efficiency measure of the security system shall be defined using the following correlations:*

$$W^{SZ} = \frac{\left\|KZ_{dop}^{SZ}\right\| - \left\|KZ_{dop}^{DSZ}\right\|}{\left\|KZ_{dop}^{SZ}\right\|} \quad (6)$$

whereas: $\left\|KZ_{dop}^{SZ}\right\|$ and $\left\|KZ_{dop}^{SZ}\right\|$ – the size of the sets of permissible security configurations.

The prerequisite $W^{SZ} = 0$ means full compliance of the set of security measures used in the security system of the organization with the set of security measures as declared in the document - "Declaration of suitability for use". The fulfillment of the above-mentioned condition shall constitute grounds for granting the information security certificate to the organization. A clear-cut advantage of the aforesaid approach is the knowledge of the method and the whole process of indicating both the set of using the security measures as well as the sets of permissible security configurations. Certainly, there is a risk that the developed method proves inefficient and the organization receives no recommendations during the certification audit, which may lead to a situation when no certificate is granted. Therefore, small companies, mainly due to the lack of human resources, decide not to develop their own methods and choose one of the solutions already available on the market, which have been approved by auditors during the certification audits.

4. Method for assessing efficiency of the security system aimed at control of the security level of information resources

To control the security level of information resources, it is indispensable to provide an entity in the security environment responsible for the decision-making process and appropriately developed procedures (steering decisions) allowing to generate proper security configurations (security processes) ensuring protection of the selected set of the information resources in the organization. The security level control also requires special security assessment and control systems as well as control of appropriate functioning of the information system in the information processing subsystem.

For the purpose of this approach, we assume that the active technical and organizational security measures shall constitute elements of the security environment of the organization [10]. The correlations between active security measures create various security configurations. The identified risks and vulnerability of the information system determine tasks that needs to be performed. The sets of risks and vulnerability change with time. The changes force other changes in the set of active security measures. The updated set of security measures makes it necessary to re-configure (mapping) the set of currently used security configurations into the set of newly generated security configurations.

A schematic representation of the reconfiguration process is in Fig. 2.

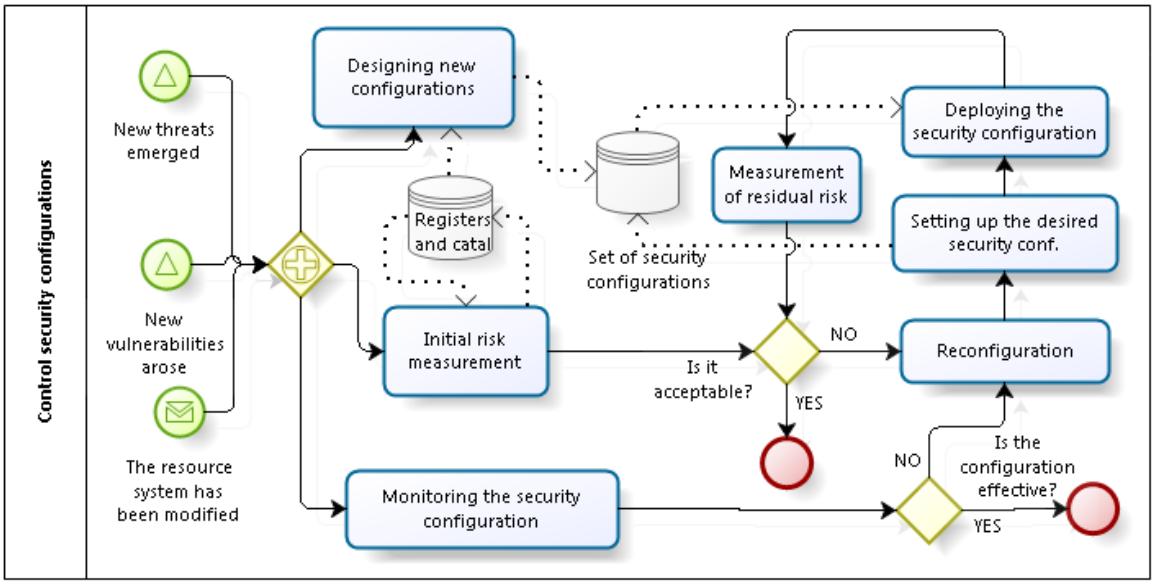

Fig. 2. Representation of reconfiguration from the point of view of controlling the security configurations.

The reconfiguration process may be represented in the following manner:

$$FR : KZ^{SZ} \longrightarrow KZ_{dop}^{SZ} \tag{7}$$

Defined as:

$$FR(KB^u) = KB^s \; where \; z, v \in N; z \neq v \tag{8}$$

where:
- N - a set of natural numbers,
- KB^u - a set of security configurations before the loss of efficiency,
- KB^s - a set of permissible security configurations.

The representation of FR shall be determined at the stage of designing the SS or establishing the Information Security Management System (ISMS) in the organization, to ensure the obtaining of the desired properties of the SS during its use.

The efficiency measure of the security system shall be defined using the following correlations [1, 2]:

$$W^{SZ} = \frac{R_p - R_k}{R_p} \tag{9}$$

where:
- R_p – the risk value by the time of starting the reconfiguration process,
- R_k – the risk value after completion of the reconfiguration process,
- whereas:

$$R_p = \sum_{z \in A} MMZ(z) \frac{\sum_{i \in AT} \frac{S_i^z}{C_i^z}}{\|A\|} \tag{10}$$

$$R_k = \sum_{z \in A} MMZ(z) \frac{\sum_{i \in AT} \frac{S_i^z}{D_i^z}}{\|A\|} \tag{11}$$

where:

1) z – a number of the information resources subject to protection by the SS,
2) A – a set of numbers of the selected resources,
3) $\|A\|$ – a number of the information resources; size of A set,
4) $MMZ(z)$ – the value assigned to a possibility of risk materialization $MMZ(z) \in \{0,1,2,3,4\}$, where:
   0 – improbable event (no risk),
   1 – almost improbable event,
   2 – quite probable event,
   3 – highly probable event,
   4 – almost certain event.
5) AT – a set of names of security attributes assigned to the particular information resources, AT= $\{P, D, I, N, R, N\}$, $i \in AT$ where: C – confidentiality, A – availability, I – integrity, N – non-repudiation, AC – accountability, R – reliability;
6) S_i^z - the value assigned to the result of the i-th attribute and z-th resource, $S_i^z \in \{0,1,2,3,4\}$, where:
   0 – no effect (no vulnerability),
   1 – insignificant effect,
   2 – significant effect,
   3 – very significant effect,
   4 – disastrous effect.
7) C_i^z – efficiency of protection against reconfiguration, $C_i^z \in \{1,2,3,4\}$, *where:*
   1 – no security measures,
   2 – security measures limit the risk,
   3 – security measures significantly limit the risk,
   4 – security measures very significantly limit the risk.
8) D – efficiency of protection after reconfiguration, $D_i^z \in \{1,2,3,4\}$, where:

1 – no security measures,
2 – security measures limit the risk,
3 – security measures significantly limit the risk,
4 – security measures very significantly limit the risk.

Summary

The general conclusion is that the information safety is very important, thus, to ensure it, it is essential to implement the efficient Information Security Management System, "driven" by a reliable security system. The information safety may be guaranteed by implementing appropriate security configurations, determined at the stage of designing the security system and tested at the stage of trail operation or internal audit. Broadly speaking, appropriately constructed and implemented technical and organizational security configurations shall: mitigate potential losses and decrease vulnerability of the resources, improve resistance to attacks (preventive measures), as they stop the emission of negative effects and may facilitate risk detection (risk identification measures). The efficient security system may not only stop the risk, but also decrease its efficiency and probability of occurrence.

The security level of the information resources of the information system in the organization is the outcome of efficiency of the selected security configurations of the SS – with respect to the set of the protected information resources and certain types of risks and vulnerability.

The sets of risks and vulnerability change with time. The changes force other changes in the set of active security measures. The updated set of security measures makes it necessary to re-configure (mapping) the set of currently used security configurations into the set of newly generated security configurations.

To maintain the desired level of security of the information system, two basic methods shall be applied [11]:

- audit of the information system, i.e. one-time or periodically repeated comprehensive assessment of the security level;
- monitoring of the information system, i.e. continuous operations aimed at supervision of the changing system, its users and environment.

The security configurations may have different functions [12, 13]. For the technical or organizational security configurations to be efficient, it is essential to design them carefully, and - after implementation - test them under the SS audit procedure.

References

[1] R. Hoffmann, M. Kiedrowicz, J. Stanik, *Risk management system as the basic paradigm of the information security management system in an organization*, MATEC Web of Conferences, vol. **76**, (2016)

[2] R. Hoffmann, M. Kiedrowicz, J. Stanik, *Evaluation of information safety as an element of improving the organization's safety management*, MATEC Web of Conferences, vol. **76**, (2016)

[3] D. Pierzchała, R. Antkiewicz, M. Dyk, R. Kasprzyk, A. Najgebauer, Z. Tarapata, *Modelling, simulation and computer support of the Polish criminal procedure*, in: *Information Systems Architecture and Technology. The Use of IT Technologies to Support Organizational Management in Risky Environment*, ed. Z. Wilimowska, L. Borzemski, A. Grzech, J. Świątek, ISBN 978-83-7493-858-7, pp. 51-60, Wrocław, (2014)

[4] Z. Tarapata, M. Zabielski, R. Kasprzyk, K. Szkółka, *Profile Cloning Detection in Online Social Networks*, Computer Science and Mathematical Modelling, vol. **3**, pp.39-46, (2016)

[5] A. Najgebauer, R. Antkiewicz, M. Chmielewski, M. Dyk, R. Kasprzyk, D. Pierzchała, J. Rulka, Z. Tarapata, *The Qualitative and Quantitative Support Method for Capability Based Planning of Armed Forces Development*, LNAI, Springer, vol. 9012, pp. 224-234, (2015)

[6] ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements. ISO, Geneva (2013)

[7] J. Stanik, M. Kiedrowicz, R. Hoffmann, Wieloaspektowa metodyka analizy i zarządzania ryzykiem procesów biznesowych, in: *Zeszyty Naukowe Uniwersytetu Szczecińskiego Ekonomiczne Problemy Usług*, Szczecin (2017)

[8] J. Krawiec, *System zarządzania bezpieczeństwem informacji – zabezpieczenia*, In: *Zeszyty Naukowe Wyższej Szkoły Informatyki, Zarządzania i Administracji w Warszawie*, vol. **15**, part **1**, p. 38, (2017)

[9] ISO/IEC 27006:2015 Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems. ISO, Geneva (2013)

[10] J. Stanik, M. Kiedrowicz, *Model ryzyka procesów biznesowych*. In: *Zeszyty Naukowe Uniwersytetu Szczecińskiego, Ekonomiczne Problemy Usług,* Szczecin (2017)

[11] J. Stanik, *Koncepcja systemu zarządzania ryzykiem w bezpieczeństwie informacji na przykładzie „Kancelarii RFID"*, In: M. Kiedrowicz (ed.) *Zarządzanie informacjami wrażliwymi. Wybrane aspekty organizacyjne, prawne i techniczne ochrony informacji niejawnych*, Warszawa (2015)

[12] PN-ISO/IEC 27005 Technika informatyczna, Techniki bezpieczeństwa. Zarządzanie ryzykiem w bezpieczeństwie informacji, PKN (2013)

[13] PN-ISO 31000:2012 Zarządzanie ryzykiem -- Zasady i wytyczne, PKN (2012)