System risk model of the IT system supporting the processing of documents at different levels of sensitivity

Jerzy STANIK[1,*]

[1] Military University of Technology, Faculty of Cybernetics, Institute of Computer and Information Systems, Warsaw, Poland

Abstract. This study outlines the system risk model of IT system oriented at the safety of the processes of sensitive data processing. The model constitutes a multi-dimensional approach to the analysis of IT system risk and IT processes implemented therein. The presented approach includes various categories of risk factors, resulting from both the architecture of the very IT system, IT security elements and security of the continued operations. The model described in this article may constitute a starting point for the development of the method for IT system risk analysis and appropriate IT security policy, which may in turn constitute input values for the methodology of IT system risk management.

Introduction

When analyzing various models, methods and approaches to assessment of the risk level and proper handling of risks, a question arises whether a possibility of creating a complex and adequate IT system risk assessment model[1], where the documents at different sensitivity levels are processed, and which includes various categories of risk factors allowing their combination so that it is possible to determine the risk level of sensitive documents, while maintaining practical usability of the proposed solution, does actually exist. This article is an attempt to answer the above question by outlining the system risk model of IT system supporting the processing of the documents different levels of sensitivity, which is - according to the authors - complete and consistent. The proposed risk model may be used at the stage of managing the IT system security and also developing the appropriate IT system security policy.

The risk related to IT systems may be considered in two different ways. Firstly, it is perceived as the design risk associated with other risks occurring at different stages of the IT system life cycle. Secondly, the approach consists in the analysis of the implemented processes of sensitive data processing to assess the risks related thereto and then in the management of the properly identified risks by accepting, transferring, avoiding or mitigating such risks. This study presents the IT system model of the office in such context. If the IT system risk level of the office is known, it is possible to efficiently manage such risk [2-6] by applying methods, methodologies and tools intended for that purpose.

1. Basic IT system risk elements

The starting point for constructing the IT system risk assessment model, as proposed in this article, reflecting systemness of the described solution, shall be the IT system security model for the office presented in Fig. 1.

The model presented in Fig. 1 covers the three following areas: security of data, security of the processes of sensitive data processing and security of the continued process operations, and is based on the following components:

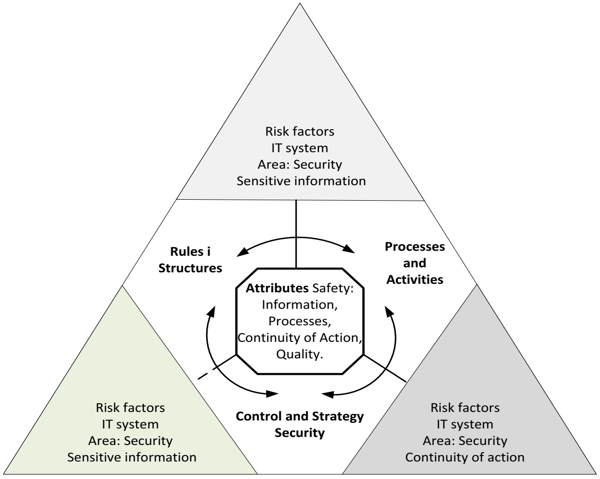

Fig. 1. The IT system security model for the office, allowing the processing of documents at different sensitivity levels.

- Rules - strategy, policies and procedures defining the rules of procedure concerning the

[*] corresponding author: jerzy.stanik@wat.edu.pl

[1] Risk assessment - the entire process of risk assessment, Risk analyses and risk evaluation. [1] definition 3.4.1.

© The Authors, published by EDP Sciences. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (http://creativecommons.org/licenses/by/4.0/).

security of sensitive data, processes of their processing and continuity of operations, whose comprehensive implementation within the entire office means efficient office management.

- Structures - a set of positions and organizational units within the organization and their correlations. For the purpose of this study, the following structures are of importance: risk management framework, security services, continued operations framework, quality and control management services.
- Office processes and operations - the solutions ensuring proper operations of the office, security and quality of the information processed therein, (Stanik i Protasowicki, 2015), compliance with the requirements on the business continuity, responses to infringement of the policies and procedures as well as incidents related to a breach of security of sensitive data.
- Security control and strategy - ongoing monitoring of the IT system operations, processes of sensitive data processing, verification of the level of compliance with safety rules as well as their consistency and adequacy, and solutions for residual risk reduction with respect to the assigned attributes of the security of the process of sensitive data processing and their business continuity.

The following correlations occur between the particular pillars of the above-described model:

- the rules included in the policies and procedures define the operations of the security solutions together with the ways of monitoring their work,
- the operations of the security systems - security-ensuring solutions - determine the occurrence of new security principles and affect the scope of the monitoring of the continued operations, whereas the quality of the processing processes determine the occurrence of new security principles and affect the scope of the monitoring and control,
- the events detected thanks to the security monitoring stimulate changes in the security solutions - security system as well as information security management system, and provide recommendations for the modifications of the existing solutions in terms of their security and creation of new security policies and procedures.

The model defined in such a manner shows the areas that determine the level of IT system risks and ensure completeness of the approach, which was confirmed by wide application of the model [7, 8]. The key element of the above-mentioned IT system security model is a set of basic IT security attributes, divided into the following subsets/areas:

I. Information security area. Within the framework of this component, the following elements with special impact on the IT system risk level may be distinguished:
   1. **Confidentiality**: Access to the information is limited to a group of authorized entities only. The data are protected against reading and copying by a person not authorized by the data owner. This type of security solution not only includes the protection of all data, but also of the individual elements thereof, which look "innocent", but may be used to breach the confidentiality of other information.
   2. **Data consistency**: The point is to ensure that the information is not modified in an unauthorized manner and that all potential modifications are detected. The information is protected against its removal or any modifications made without the consent of its owner. The protected information also includes such elements as settlement system records, tapes with back-up copies, times of creating files and documents.
   3. **Data availability**: The information may be accessed in any circumstances permitted by the information security policy. The offered services are protected against distortion and damage. If an authorized user needs to use the IT system, which is unavailable, the effect may be the same as in case of removing data from the system.
   4. **Data certainty:** The party undertaking some actions using the software may not deny the fact the (s)he performed some operations with the use of the software.

II. The area of the process of sensitive data processing. Within the framework of this component, the following elements with special impact on the IT system risk level may be distinguished:
   1. **Availability of the process of sensitive data processing** - a possibility of making a certain action in office available for use at a certain time and upon request of an authorized entity.
   2. **Operating safety**: The point is to ensure that the work of the IT system is in line with the users' expectations. If the IT system resources, e.g. hardware and software start operating significantly different than usually, especially after the software upgrade or removing hardware failure, a real disaster could happen (e.g. ls command, which starts removing files from time to time instead of displaying them). This type of protection may be considered a way of ensuring operating safety.
   3. **Process control**: The objective is to control access to the core IT system process. Unknown or unauthorized persons (or programs) in the system may constitute a serious problem. It is essential to learn how they got into the system. To remove the effects of such incidents may require substantial contribution in terms of time and workload, for example, related to the necessity of redesigning and reinstalling the

system as well as verifying whether any important component was changed or disclosed - even if nothing has actually happened.

4. **Audit:** The system is not only under threat from the unauthorized users. Sometimes authorized users make mistakes, commit offenses and even deliberately destroy things. In such case, it is important to check what was done, by whom and with what effects. One way to obtain such information is to use the damage-proof event records in the system, which allows identifying the offenders and their actions. In some critical applications, it is possible to undo certain operations, which may be helpful in the process of restoring proper condition of the system.

III. The area of the process of safety of sensitive data processing. Within the framework of this component, the following elements with special impact on the IT system risk level may be distinguished:

1. Fulfillment of the requirements included in the policy referring to the process continuity of operations,
2. Business Continuity Plan - BCP
3. Disaster Recovery Plan - DRP.
4. Financial effects of suspension/interruption of the process implementation,
5. Non-financial effects of suspension/interruption of the process implementation,
6. Costs and time of the process unavailability.

Among from the information security attributes, all of them were directly incorporated into the system risk model of IT system proposed in this article. The impact of confidentiality and availability on the IT system risk depends on the expected level of such attributes for a given system. If the expectations concerning availability or confidentiality of the IT system are high, a given attribute shall significantly affect the risk assessment process for such system. However, if the availability or confidentiality for a certain IT system is not a critical factor, then the impact of a given attribute on the risk of such IT system shall be marginal [12-13].

According to the authors, in case of attributes of the security of the processes of sensitive data processing, it is important to prevent the situations when the lack of integrity and continuity of business processes or information processed thereunder is knowingly accepted. Therefore, it may be assumed that the expectations for every process in terms of its integrity are comparable.

The *Rules*, presented in the model in Fig. 1, are characterized by the following elements having impact on the risk level of IT systems: · security policy, · security procedures, · – BCP (*Business Continuity Plan*) – DRP (*Disaster Recovery Plan*). Of these, the security policy and safe use procedures implemented in the office have key impact on the IT system risk. However, the manner of considering such factors in the presented model differs [9-11]. The security policy constitutes a direct component of the IT system risk in the proposed model, whereas the safe use procedures have only indirect impact on such risk. Since verification of the security procedures constitutes an integral part of the process of classifying IT systems and assigning them to appropriate safety classes, the impact of the security procedures on the IT system risk in the proposed model is expressed by assigning the IT system to a specific security class. The methodology proposed in this article does not include any evaluation of the BCP or DRP Plans. It is due to the fact that the BCP-related issues are more connected with business risk than IT system risk, whereas DRP is directly linked to the attribute of the IT system availability. Furthermore, practical experience has shown that IT systems not requiring high level of availability usually do not have any dedicated DRP Plans, which usually results from the economic account of profitability. Therefore, to include the IT system risk analysis in the method proposed herein, the DRP-related component, would raise the risk level of such systems. Another argument in favor of exclusion of the DRP-related component from this methodology is close connection of the DRP Plans with the business needs of a given organization. According to the author, evaluation of such plans in isolation from the business needs of the organization would be an abuse and would undermine the objectivity of the methodology proposed herein.

The category *Processes and Actions* in the model presented in Fig. 1 includes the following elements, which may have impact on the risk level of IT systems: protection processes, change management process, control and security mechanisms. The impact of the protection processes on the IT system risk, in particular its process of sensitive data processing is shown in Fig. 2. The impact of the change management process on the IT system risk is visible in commonly applied international standards, such ITIL and COBIT (Control Objectives for Information and Related Technology), which is reflected in the fact that the change management process is included in the proposed model as a risk component.

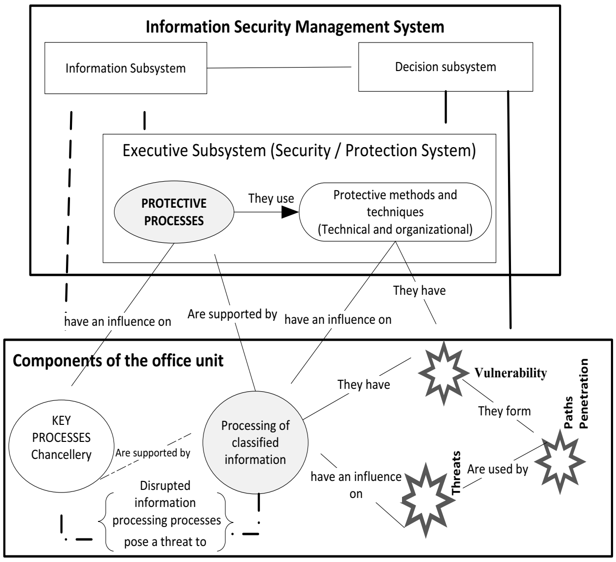
Information Security Management System
Information Subsystem
Decision subsystem
Executive Subsystem (Security / Protection System)
PROTECTIVE PROCESSES
They use
Protective methods and techniques (Technical and organizational)
They have
have an influence on
Are supported by
have an influence on
Components of the office unit
They have
Vulnerability
They form
Paths Penetration
KEY PROCESSES Chancellery
Are supported by
Processing of classified information
have an influence on
Threats
Are used by
Disrupted information processing processes pose a threat to

Fig. 2. The place of the protection processes in the information security management system in the office.

The control is the last of the main components of the IT system security model presented in Fig. 1. As part of this component, the following elements with special impact on the level of IT system risk may be distinguished: complexity of ICT environment, security monitoring system, physical and logical access control, impact of human factor. All of the above-mentioned elements are included in the method of IT system risk analysis proposed herein, however, the manner of their incorporation into the said method is different [14-19].

2. Components of the vector of IT system risk in the office

The system risk model of IT system for the office, presented herein, has been defined as the following vector $\overrightarrow{R_{S_i}}$:

$$\overrightarrow{R_{S_i}} = \langle \overrightarrow{R^B_{S_i}},\ \overrightarrow{R^C_{S_i}},\ \overrightarrow{R^T_{S_i}} \rangle \qquad (1)$$

defining the IT system risk level, which includes three composition (coordinates) partial vectors $\overrightarrow{R^B_{S_i}}$, $\overrightarrow{R^C_{S_i}}$, $\overrightarrow{R^T_{S_i}}$, reflecting the levels of IT system risks in terms of particular areas of risk factors. The selected coordinates of the risk vector represent individual risk areas (Fig. 1), each of them including several risk factors, hereinafter referred to as the composition of partial vectors of IT system risk. The components of particular partial vectors used in this IT system risk model of the office are the following:

I. Information security area - $\mathrm{R^B_{S_i}}$:

1. Data availability in the system - $\boldsymbol{\lambda_{S_i}}$**.** The data availability in the IT system S_i is a possibility of making a certain action in office available for use at a certain time and upon request of an authorized entity. The data availability in the IT system S_i is expressed by assigning the system to a particular availability class $\lambda \in \Lambda$, marked as λ_{P_i}. Set L = {I, II, III, IV, V}[2] containing the following elements is called the group of availability classes of the IT system:

   I – defines the IT system S_i, in case of which the expected availability is 99.99% per year and its maximum one-time unavailability does not exceed 30 minutes,

   V – defines the IT system S_i, in case of which the expected availability is 70% per year and its maximum one-time unavailability exceeds 3 weeks**.**

   Every IT system $S_i \epsilon P(O)$ $i \epsilon \{1, 2, \dots N\}$belongs to one and only one availability class $\lambda \in \Lambda$. The described principle of assigning the IT system S_i to a given availability class ensures explicitness of defining the availability of the IT system S_i, which is significant for the model outlined in this article.

2. Data confidentiality - α_{P_i}

The property of data non-disclosure to any unauthorized parties S_i is the IT system data confidentiality. The confidentiality of data processed by the IT system S_i is expressed by assigning the system to a particular data confidentiality class, $\alpha \epsilon$A and marked as α_{P_i}. Every IT system $S_i \epsilon P(O)$ $i \epsilon \{1, 2, \dots N\}$ belongs to one and only one availability class of confidentiality of the business process data $\alpha \in A$. The set of confidentiality classes of data processed by the IT system S_i is called A = {A, B, C, D, E}, composed of the following elements:

A – defines the IT system and processes secret data, whose disclosure may pose threat to human life or health,

E – defines the IT system, used for processing of public data.

3. Fulfillment of the requirements defined in the information security policy -$\eta^{\mathrm{B}}_{\mathrm{S_i}}$. The set of requirements in the O's office security policy is a finite set, $W^B_{P(O)} = \{w_{1,} w_{2,} \dots w_{\mathrm{m},} \dots w_{\mathrm{M^B}}\}$, where: M^B is the number of requirements in the security policy in terms of P(O). In case of each requirement, $w_m \epsilon W^B_{P(O)}$ we define the priority of the requirement in terms of a given IT system S_i. The requirement priority $w_m \epsilon W^B_{P(O)}$ in terms of the IT system S_i is the number $p^m_{S_i} \in \{0,1, \dots 5\}$, where:

0 – means that the requirement is inaccurate for the IT system S_i,

5 – means that the requirement is maximally significant for the system S_i.

The values from 1 to 5 are numerical expressions of the following: minimum, low, medium, high and maximum level of significance of the requirement in terms of a given IT system. To allow 0 value in the set of values $p^m_{S_i}$ means to respond to the situations, when the requirement has nothing to do with the analyzed IT system. Therefore, in case of each IT system $S_i \epsilon P(O)$, there is the following set: $W^B_{S_i}$such as that: $W^B_{S_i} \neq \emptyset$, $W^B_{S_i} \subseteq W_{P(O)}$, $w_m \epsilon W^B_{P(O)}$ belongs to $W^B_{S_i}$ when and only when $p^m_{P_i} \neq 0$.

The fulfillment of the requirement $w_m \epsilon W^B_{P(O)}$of the IT system S_i is the number, $s^m_{P_i} \in [0\%, \dots, 100\%]$, where 0% – means that the requirement has not been met in terms of the process P_i, 100% – means that the requirement has been fully met in terms of the process P_i. The fulfillment of the requirements

[2] While considering the subjectivity of interpretations of particular elements in the group of availability classes and limited number of pages in this articles, I have decided to include construction of only two extreme elements of the particular sets.

of the IT system policy S_i is the following percentage value:

$$\eta^B_{S_i} = \frac{\sum_{m=1}^{\overline{W^B_{P(O)}}} \left(p^m_{S_i} * s^m_{S_i}\right)}{\sum_{m=1}^{\overline{W^B_{P(O)}}} p^m_{S_i}} \qquad (2)$$

where:

- $W^B_{S_i}$ – the set of system requirements S_i,
- $p^m_{S_i}$– the priority of *m* system requirement S_i,
- $s^m_{S_i}$ – the fulfillment of *m* system requirementS_i,

4. *Efficiency of the system monitoring of the information security*– $\beta^B_{S_i}$,

The efficiency of the system monitoring of the data for the IT system S_i is in the form of the following product:

$$\beta^B_{S_i} = d^B_{SM}(S_i) * \sum_j \left(\delta^m_{S_i} * v^{kj}_{S_i}\right); \qquad (3)$$

where:

j – the number of the next criterion for assessing efficiency of the security monitoring system,

$\delta^m_{S_i}$– priority of the *j–th* criterion for assessing efficiency of the system security monitoring systemS_i,

$v^{kj}_{S_i}$– value of the *j–th* criterion for assessing efficiency of the system security monitoring systemS_i,

k^j – materiality of the *j–th* criterion for assessing efficiency of the system security monitoring system,

$d^B_{SM}(S_i)$– multiplier of the inclusion of the IT system S_i in the security monitoring system, whereas:

$$d^B_{SM}(S_i) = \begin{cases} 1, \text{if the IT system is covered by a monitoring system to monitor the information system} \\ 0, \text{if the IT system is not covered by a monitoring systemto monitor the information system} \end{cases}$$

If the IT system S_i is under various monitoring systems, it is essential to define the number of criteria for assessing efficiency of such monitoring systems, e.g. in the form of tables [Table 1].

Table 1. Sample criteria for assessing efficiency of the security monitoring systems

Criterion	Priority $\delta^m_{P_i}$	Materiality k^j	Value $v^{kj}_{P_i}$
Journal of process operations (collection of logs and data archivization)	4	3	{0,1,2,3,4,5}, where: 0 – no journal of the process operations (collection of logs) and no data archivization are made; 5 – efficient, modern and reliable backup mechanisms as well as log and data archivization are implemented for the process;
Analysis of susceptibility to frauds	3	2	{0,1,2,3,4,5}, where: 0 – no mechanisms of susceptibility analysis; 5 – developed system of susceptibility analysis, detecting possible susceptibility of business processes as well as offering certain ways of removing detected gaps and supporting the process of their removal;
Reactions related to detection of frauds	3	3	{1,2}, where: 2 - allows to automatically react to an attack; 1 - sends notifications about the detected events and undertaken actions; 1 - allows interruption of suspicious sessions and processes; 2 - allows separation of the attack source from the remaining part of the ICT infrastructure;

Average time of the system's reactions to an event (from the time of occurrence of such event to the time of its reporting and starting potential automatic reactions)	4	3	{0,1,2,3,4,5}, where:
			0 – over 1 hour;
			1 – from 5 minutes up to 1 hour;
			2 – from 30 seconds up to 5 minutes;
			3 – from 5 seconds up to 30 seconds;
			4 – from 1 second up to 5 seconds;
			5 – up to 1 second;

Reporting and data analysis	3	1	{0,1,2,3,4,5}, where: 1 – the system offers basic functionalities related to reporting; 5 – the system has a developed data warehouse module, allowing to perform multidimensional analyses according to the predefined criteria;

Source: own elaboration.

Otherwise, in compliance with the above definitions, the efficiency of the monitoring system selected for the IT system S_i would be zero and further determination of its parameters - unjustified. The criteria presented in Table 1 with respect to assessment of the monitoring system efficiency, materiality values and priorities of particular criteria as well as sets of their available values are not obligatory and may be customized. They should be considered sample data. The point of the above-described method for assessing efficiency of the security monitoring systems is to describe, in a quantitative manner, the quality rate of a given system that would allow direct comparison of the security monitoring systems from different supplier and characterized by different qualitative, functional and operational parameters.

II. Business continuity operations area - $\mathbf{R^C_{S_i}}$:

1. Fulfillment of the requirements defined in the business continuity management policy - $\eta^C_{S_i}$

The set of requirements in the O' office BC policy is a set, $W^C_{P(O)} = \{w_1, w_2, \dots w_m, \dots w_{M^C}\}$, where: M^C is the number of requirements in the security policy in terms of P(O). In case of each requirement, $w_m \epsilon W^C_{P(O)}$ we define the priority of the requirement in terms of a given IT system S_i. The requirement priority $w_m \epsilon W^C_{P(O)}$ in terms of the IT system S_i is the number $p^m_{S_i} \in \{0,1, \dots 5\}$, where:

0 – means that the requirement is inaccurate for the IT system S_i,

5 – means that the requirement is maximally significant for the system S_i.

The values from 1 to 5 are numerical expressions of the following: minimum, low, medium, high and maximum level of significance of the requirement in terms of a given IT system. To allow 0 value in the set of values $p^m_{S_i}$ means to respond to the situations, when the requirement has nothing to do with the analyzed IT system. Therefore, in case of each IT system $S_i \ \epsilon P(O)$, there is the following set: $W^C_{S_i}$such as that: $W^C_{S_i} \neq \emptyset$, $W^C_{S_i} \subseteq W_{P(O)}$, $w_m \epsilon W^C_{P(O)}$ belongs to $W^C_{S_i}$ when and only when $p^m_{P_i} \neq 0$.

The fulfillment of the requirement $w_m \epsilon W^C_{P(O)}$of the IT system S_i is the number, $s^m_{P_i} \in [0\%, \dots, 100\%]$, where 0% – means that the requirement has not been met in terms of the process P_i, 100% – means that the requirement has been fully met in terms of the process P_i. The fulfillment of the requirements in the business continuity management policy of the IT system S_i is the following percentage value:

$$\eta^B_{S_i} = \frac{\sum_{m=1}^{\overline{\overline{W^C_{P(O)}}}} \left(p^m_{S_i} * s^m_{S_i}\right)}{\sum_{m=1}^{\overline{\overline{W^C_{P(O)}}}} p^m_{S_i}} \qquad (4)$$

where:

- $W^C_{S_i}$ –the set of business continuity requirements of the system S_i,
- $p^m_{S_i}$– the priority of *m* system requirement S_i,
- $s^m_{S_i}$ – the fulfillment of *m* system requirement S_i,

2. Efficiency of the system monitoring the business continuity $- \beta^C_{S_i}$

The efficiency of the system monitoring the business continuity of the IT system S_i is in the form of the following product:

$$\beta^C_{S_i} = d^C_{SM}(S_i) * \sum_j \left(\delta^m_{S_i} * v^{k^j}_{S_i}\right); \qquad (5)$$

where:

j – the number of the next criterion for assessing efficiency of the system monitoring the business continuity,

$\delta^m_{S_i}$– priority of the *j–th* criterion for assessing efficiency of the system security monitoring the system's business continuity S_i,

$v^{k^j}_{S_i}$– value of the *j–th* criterion for assessing efficiency of the system security monitoring the system's business continuity S_i,

k^j – materiality of the *j–th* criterion for assessing efficiency of the system monitoring the business continuity,

$d^C_{SM}(S_i)$– multiplier of the inclusion of the IT system S_i in the system monitoring the business continuity,

whereas:

$$d^C_{SM}(S_i) = \begin{cases} 1, if \text{ the IT system is covered by a monitoring} \\ \quad \text{system to monitor the information system} \\ 0, \text{if the IT system is not covered by a monitoring} \\ \quad \text{systemto monitor the information system} \end{cases}$$

BCP (Business Continuity Plan) and DRP (Disaster Recovery Plan).

The model proposed in this article does not include any evaluation of the BCP or DRP Plans. It is due to the fact that the BCP-related issues are more connected with business risk than IT system risk, whereas DRP is directly linked to the attribute of the IT system availability. Furthermore, practical experience has shown that the IT systems implemented in the office, i.e. RFID, which do not require high level of availability, usually do not have any dedicated DRP Plans, which usually results from the economic account of profitability. Therefore, to include the IT system risk in the model proposed herein, the DRP-related component, would raise the risk level of such systems. Another argument in favor of exclusion of the DRP-related component from this model is close connection of the DRP Plans with the business needs of a given organization. According to the author, evaluation of such plans in isolation from the business needs of the organization would be an abuse and would undermine the objectivity of the methodology proposed herein.

3. Cost of the IT system unavailability -κ_{S_i}

The costs related to unavailability of the IT system include all expenses connected with the performance of a given portion of actions, i.e. the operations that constitute a specific information process. To estimate the costs of the IT system unavailability, it was assumed that the event causing interruption of the information processing may occur at the worst possible moment. The cost of the IT system unavailability S_i is the measure consisting of financial effects of the interrupted process and non-financial effects of suspended information processing. The financial effects of the interrupted process of sensitive data processing shall be deemed to mean maximum potential financial losses that the Office would incur due to the suspension of such process for a definite time. The financial effects may be as follows: loss of profits, contractual damages, penalty interest, fines, potentially additional costs of running the office. The non-financial costs of suspending the processes are the consequences of the suspended processed, which may not be expressed by the volume of losses. The materiality of the non-financial effects of the suspended process for a definite time is estimated by choosing one of the following levels:

- insignificant effects - unnoticeable effects or no effects,
- noticeable effects - visible effects, in case of which no actions are required,
- serious effects - effects requiring certain actions to be undertaken for the purpose of their removal,
- very serious effects - effects requiring certain actions to be undertaken for the purpose of preventing discontinuance of business operations of the whole company,
- catastrophic effects - effects that may directly lead to the company's fall.

The non-financial effects are as follows:

- potential loss of trust on the market, e.g. loss of partners' trust, loss of the office's goodwill, dissatisfaction of clients, loss of clients,
- potential legal consequences (other than financial), e.g. restraint of liberty,
- potential dissatisfaction of the company's owners,
- potential dissatisfaction of individual clients,
- potential impediment to the activities of business, e.g. inability or problematic implementation of another process in the office.

The cost of unavailability of the process of information processing is expressed by assigning the process to a particular unavailability cost class $\kappa \in$ K, marked as κ_{S_i}. Set K = {I, II, III, IV, V, VI} containing the following elements is called the group of unavailability classes of the business processes:

I – defines the process of sensitive data processing, in case of which the level of financial costs does not exceed 5% of the office's financial fluidity ratio, e.g. 1 000, whereas the level of the non-financial costs is insignificant; VI – defines the process of sensitive data processing, in case of which the level of financial costs exceeds 50% of the office's financial fluidity ratio, e.g. 1 000 000, whereas the level of non-financial costs is catastrophic.

Every process of sensitive data processing $P_i \epsilon P(O)$ $i\epsilon\{1, 2, \dots N\}$belongs to one and only one unavailability cost class. $\kappa \in$ K. The proposed scale is not obligatory, may be customized.

4. The maximum time of unavailability of the processes of sensitive data processing - π_{S_i}

   Maximum time of the process unavailability is the time during which the process execution must be restored to prevent any significant financial or non-financial effects. The maximum time of unavailability of the processes of information processing is expressed by assigning the process to a particular unavailability time class $\pi \in \Psi$ and is marked as π_{S_i}. The group of unavailability time classes of the *process of sensitive data processing* is set N = {0,1,2,3,4,5}, where: 0 – less than 1 hour; 1 – 4 hours; 2 – 1 day; 3 - 1 week, 4 – more than 1 week, 5 - 1 month and more.

   Every process of sensitive data processing $P_i \epsilon P(O)$, $i\epsilon\{1, 2, \dots \mathrm{T}\}$, belongs to one and only one cost class of the process of sensitive data processing. $\pi \in \Psi$. The proposed scale is not obligatory, may be customized.

III. Processing security area - $\mathrm{R}^{\mathrm{T}}_{\mathrm{S_i}}$:

1. Fulfillment of the requirements defined in the processing security policy - $\eta^T_{S_i}$

   The set of requirements in the O's office processing security policy is a finite and countable set, $W^T_{P(O)} = \{w_{1,}w_{2,} \dots w_{\mathrm{m},} \dots \mathrm{w}_{\mathrm{M}^T}\}$, where: M^T it is the number of requirements of the security policy with respect to the processing processes $P_j \epsilon S_i \in P(O)$. In case of each requirement, $w_m \epsilon W^T_{P(O)}$ we define the priority of the requirement in terms of a given IT system S_i. The requirement priority $w_m \epsilon W^T_{P(O)}$ in terms of the IT system S_i is the number $p^m_{S_i} \in \{0,1, \dots 5\}$, where:

   0 – means that the requirement is inaccurate for the IT system ; S_i,

   5 – means that the requirement is maximally significant for the system S_i.

The values from 1 to 5 are numerical expressions of the following: minimum, low, medium, high and maximum level of significance of the requirement in terms of a given IT system. To allow 0 value in the set of values $p^m_{S_i}$ means to respond to the situations, when the requirement has nothing to do with the analyzed IT system. Therefore, in case of each IT system S_i $\epsilon P(O)$, there is the following set: $W^T_{S_i}$ such as that:$W^T_{S_i} \neq \emptyset$, $W^J_{S_i} \subseteq W_{P(O)}$, $w_m \epsilon W^T_{P(O)}$ belongs to $W^T_{S_i}$ when and only when $p^m_{P_i} \neq 0$. The fulfillment of the requirement $w_m \epsilon W^T_{P(O)}$of the IT system S_i is the number, $s^m_{P_i} \in [0\%, \dots, 100\%]$, where 0% – means that the requirement has not been met in terms of the process P_i, 100% – means that the requirement has been fully met in terms of the process P_i. The fulfillment of the requirements in the business continuity management policy of the IT system S_i is the following percentage value:

$$\eta_{S_i}^T = \frac{\sum_{m=1}^{\overline{W_{P(O)}^T}} \left(p_{S_i}^m * s_{S_i}^m\right)}{\sum_{m=1}^{\overline{W_{P(O)}^T}} p_{S_i}^m} \qquad (6)$$

where:

- $W_{S_i}^T$ –the set of business continuity requirements of the system S_i,
- $p_{S_i}^m$– the priority of m system requirement S_i,
- $s_{S_i}^m$ – the fulfillment of m system requirement S_i,

2. Efficiency of the quality monitoring system – $\beta_{S_i}^T$

The efficiency of the quality monitoring system for the IT system S_i is in the form of the following product:

$$\beta_{S_i}^T = d_{SM}^T(S_i) * \sum_j \left(\delta_{S_i}^m * \upsilon_{S_i}^{k^j}\right); \qquad (7)$$

where:

j – the number of the next criterion for assessing efficiency of the quality monitoring system,

$\delta_{S_i}^m$ – priority of the *j–th* criterion for assessing efficiency of the quality monitoring systemS_i,

$\upsilon_{S_i}^{k^j}$– value of the *j–th* criterion for assessing efficiency of the quality monitoring systemS_i,

k^j – materiality of the *j–th* criterion for assessing efficiency of the quality monitoring system,

$d_{SM}^T(S_i)$– multiplier of the inclusion of the IT system S_i in the quality monitoring system, whereas:

$$d_{SM}^T(S_i) = \begin{cases} 1, if \text{ the IT system is covered by a monitoring system to monitor the information system} \\ 0, \text{if the IT system is not covered by a monitoring systemto monitor the information system} \end{cases}$$

3. Duration of information processing - δ_{S_i}

It is the average time of all operations related to the information processing. The duration mainly depends on the organizational level of the implemented procedures and value added level. The time of the sensitive information processing is expressed by assigning the process to a particular execution time class $\delta \in \Delta$, marked as δ_{S_i}. The group of execution time classes of the *process of data processing* is set Δ = {0,1,2,3}, where: 0 – insignificant; 1 – medium organizational level of the implemented procedures and low value added; 2 – medium organizational level of the implemented procedures and average value added; 3 – high organizational level of the implemented procedures and high value added.

Every process of sensitive data processing $P_i \in P(O)$, $i\epsilon\{1, 2, \ldots \mathrm{L}\}$, belongs to one and only one cost class of the process of sensitive data processing. $\delta \in \Delta$. The proposed scale is not obligatory, may be customized.

4. Processing flexibility in the IT system - ϑ_{S_i}

The processing flexibility in the IT system $\mathrm{S_i}$ means the process ability to change, update, change order of the performed actions, merge operations, etc. It $\mathrm{S_i}$ is also determined on the basis of the process susceptibility to the transformation of the used resources as well as the speed rate of responding to the clients' requests. To introduce the definition of the processing flexibility scales in the IT system, $\mathrm{S_i}$ the following definitions have been adopted. The group of the processing flexibility scale classes $\mathrm{S_i}$ constitutes set E = {0,1,..,9}, whose elements discretize the processing flexibility scale in the IT system $\mathrm{S_i}$, where: 0 – no processing flexibility in the IT system $\mathrm{S_i}$, 9 – processing flexibility in the IT system $\mathrm{S_i}$, with maximum reach, but at variance with the scope of requirements adopted in the security and business continuity policies. The proposed scale is not obligatory, may be customized. The level of the distribution and multiplicity of the IT system architecture components is called the scale of the processing process in the IT system$\mathrm{S_i}$. The scale of the processing flexibility in the IT system $\mathrm{S_i}$ is expressed by assigning the system to a particular flexibility scale class $\vartheta \in \Theta$, marked as $\vartheta_{\mathrm{P_i}}$.

5. Importance of the IT system - $\zeta_{\mathrm{S_i}}$

The importance of the IT system$\mathrm{S_i}$ is the measure consisting of the consumer and recipient satisfaction levels, amounts of revenue generated by the system, strength of relationships between the system and clients. The importance of the IT system S_i is expressed by assigning the system to the importance class $\zeta \in \mathrm{Z}$ and marked $\zeta_{\mathrm{S_i}}$. Set ZN = {I, II, III, IV, V,VI}S_i containing the following elements is called the group of the IT system importance classes: I – defines the IT system S_i, in case of which the consumer satisfaction level is below 50% and the amount of revenue generated by the system is low, VI - defines the IT system S_i, in case of which the consumer satisfaction level is over 90% and the amount of revenue generated by the system is very high. Every IT system $\mathrm{S}_i \in \mathrm{P(O)}$ $\mathrm{i} \in \{1, 2, \ldots \mathrm{Z}\}$ belongs to one and only one IT system importance class. $\zeta \in \mathrm{Z}$.

6. Efficiency of the change management process - φ_{P_i}

The efficiency of the change management process is the level of compliance of such process in the IT system S_i with the best practices in that respect. The efficiency of the change management process in the IT system S_i is expressed by way of the percentage compliance of such process S_i with the ITIL or other standards in that respect. The efficiency of the change management process in the IT system S_i is marked as φ_{P_i}.

3. Normalized components of the IT system risk vector

Due to the fact that the particular coordinates of the IT system risk vector as well as individual risk factors belong to different sets of values, it is necessary to introduce the function ξ or group of functions$\xi\epsilon\Xi$, which would clearly transpose the components to the uniform range of values. The standardization function is the family of functions $\xi: X \longrightarrow [1, 2, \ldots, N]$. Various forms of the standardization function from the family Ξ should be defined in such a manner so that they reflect their values per range [1,..., *N*] and maintain appropriate proportions of their impact on total IT system risk, including the set X of all specialized risk factors divided into subsets X^B, X^T, X^C representing the elected areas/aspects: information security, processing security and business continuity regarding the processing of sensitive information. Another limitation is to express the numbers L^B, L^T, L^C of the selected standardization function from the family Ξ as a product of two natural numbers larger than 1 is another limitation, i.e.:

$$\|\Xi^B\| = L^B = m \times n, m > 1, n > 1, \Xi^B \subset \Xi$$
$$\|\Xi^T\| = L^T = m \times n, m > 1, n > 1, \Xi^T \subset \Xi$$
$$\|\Xi^C\| = L^C = m \times n, m > 1, n > 1, \Xi^C \subset \Xi$$

Furthermore, the point is to make the products: $L^B \times N^B, L^T \times N^T, L^C \times N^C \cong 100$, then the calculated length of the IT system risk vector $\overrightarrow{R_{S_i}}$ and its coordinates $\left(\overrightarrow{R^B_{S_i}}, \overrightarrow{R^C_{S_i}}, \overrightarrow{R^T_{S_i}}\right)$ may be measured as scaled percentages and hence may be easily interpreted.
In the model proposed herein, the following values have been adopted:

- Information security area: $L^B = 4$, N^B=24, $\xi: X^B \longrightarrow [1, 2, \ldots, 24]$ *and* $L^B \times N^B \cong 100$
- Process security area: $L^T = 6$, N^T=16, $\xi: X^T \longrightarrow [1, 2, \ldots, 8]$ *and* $L^T \times N^T \cong 100$
- Business continuity area: L^C =4, N^C=24 $\xi: X^C \longrightarrow [1, 2, \ldots, 24]$ *and* $L^C \times N^C \cong 100$.

The proposed ranges are not obligatory, may be customized. Such value ranges are aimed at creating the simplest possible shape of the functions that would transpose particular coordinates of the vector $\overrightarrow{R_{S_i}}$ and components of the described model into uniform value ranges, additionally ensuring legibility of the risk analysis results. The exclusion of the values lower than 1, in particular 0 values, from such range is associated with the concept of a residual risk, (Hash, 2002), according to which it is impossible to completely eliminate the risk, thus, none of its components presented in the IT system risk model may have zero value. To transpose the values of the individual IT system risk components into the uniform value ranges, we have introduced the concept of the standardization function.

When considering the above assumption and limitations, the standardization functions $\xi\epsilon\Xi$ shall be as follows:

A. in case of a subset of the functions $\xi\epsilon\Xi^B$ characterized by the information security:

1. for the data *availability* component, it is defined in the following manner:

$$\xi_\lambda(\lambda_{S_i}) = \begin{cases} 1,\ if\ \lambda_{S_i} = \mathrm{V} \\ 7, if\ \lambda_{S_i} = IV \\ 13, if\ \lambda_{S_i} = III \\ 19, if\ \lambda_{S_i} = II \\ 24, if\ \lambda_{S_i} = I \end{cases}; \tag{8}$$

2. for the data confidentiality component, it is defined in the following manner:

$$\xi_\alpha(\alpha_{S_i}) = \begin{cases} 1,\ if\ \alpha_{S_i} = E \\ 7, if\ \alpha_{S_i} = D \\ 13, if\ \alpha_{S_i} = C \\ 19, if\ \alpha_{S_i} = B \\ 24, if\ \alpha_{S_i} = A \end{cases}; \tag{9}$$

3. for the component concerning the fulfillment of the requirements of the information security policy, it is defined in the following manner: $\eta^B_{S_i}$,

$$\xi^B_\eta(\eta^B_{S_i}) = 1 + 23 * \left(1 - \frac{\eta^B_{S_i}}{100\%}\right); \tag{10}$$

4. for the information security monitoring component, it is defined in the following manner: $\beta^B_{S_i}$,

$$\xi^B_\eta(\beta^B_{S_i}) = 24 - \sqrt[3]{\frac{\beta^B_{S_i}}{2}}; \tag{11}$$

B. in case of a subset of the functions $\xi\epsilon\Xi^C$ characterized by the business continuity security of the process of sensitive data processing:

1. for the component concerning the fulfillment of the requirements of the business continuity security of the process of sensitive data processing, it is defined in the following manner: $\eta^C_{S_i}$,

$$\xi^C_\eta(\eta^C_{S_i}) = 1 + 23 * \left(1 - \frac{\eta^C_{S_i}}{100\%}\right), \tag{12}$$

2. for the component concerning the business continuity security of the process of sensitive data processing in the IT system, it is defined in the following manner: $\beta^C_{S_i}$

$$\xi^C_\beta(\beta^C_{S_i}) = 24 - \sqrt[3]{\frac{\beta^C_{P_i}}{2}}, \tag{13}$$

3. for the component concerning the costs due to unavailability of the processing processes in the IT system, it is defined in the following manner: κ_{S_i}

$$\xi_\kappa(\kappa_{S_i}) = \begin{cases} 1, if\ \kappa_{S_i} = V \\ 7, if\ \kappa_{S_i} = IV \\ 13, if\ \kappa_{S_i} = III; \\ 19, if\ \kappa_{S_i} = II \\ 24, if\ \kappa_{S_i} = I \end{cases} \qquad 14)$$

4. for the maximum unavailability time component, it is defined in the following manner: π_{S_i}

$$\xi_\pi(\pi_{S_i}) = \begin{cases} 1, if\ \pi_{S_i} = 4 \\ 7, if\ \pi_{S_i} = 3 \\ 13, if\ \pi_{S_i} = 2; \\ 19, if\ \pi_{S_i} = 1 \\ 24, if\ \pi_{S_i} = 0 \end{cases} \tag{15}$$

C. in case of a subset of the functions $\xi \epsilon \Xi^T$ characterized by the security of the processes of sensitive data processing:

1. for the component concerning the fulfillment of the requirements of the information processing security policy, it is defined in the following manner: $\eta_{S_i}^T$,

$$\xi_\eta^T(\eta_S^T) = 1 + 15 * \left(1 - \frac{\eta_{S_i}^T}{100\%}\right); \tag{16}$$

2. for the component concerning the monitoring of the security of the processing processes in the IT system, it is defined in the following manner: $\beta_{S_i}^T$,

$$\xi_\eta^T(\beta_{S_i}^T) = 16 - \sqrt[3]{\frac{\beta_{S_i}^T}{2}}; \quad , \tag{17}$$

3. for the component concerning the duration of the information processing, it is defined in the following manner: δ_{S_i}

$$\xi_\delta(\delta_{S_i}) = $$
$$\begin{cases} 1, when\ there\ is\ lack\ of\ system\ flexibility \\ 5, when\ the\ flexibilityof\ the\ system\ is\ low \\ 10, when\ the\ flexibility\ of\ the\ system\ is\ good \\ 15, when\ the\ flexibility\ of\ the\ system\ is\ maximum \end{cases}$$

4. for the system *flexibility* component, it is defined in the following manner: ϑ_{S_i}

$$\xi_\vartheta(\vartheta_{S_i}) = \begin{cases} 1, if\ \vartheta_{S_i} = 4 \\ 7, if\ \vartheta_{S_i} = 3 \\ 13, if\ \vartheta_{S_i} = 2; \\ 19, if\ \vartheta_{S_i} = 1 \\ 24, if\ \vartheta_{S_i} = 0 \end{cases} \tag{18}$$

5. for the system importance component, it is defined in the following manner: - ζ_{S_i}

$$\xi_\zeta(\zeta_{S_i}) = \begin{cases} 1, if\ \zeta_{S_i} = VI \\ 4, if\ \zeta_{S_i} = V \\ 7, if\ \zeta_{S_i} = IV \\ 10, if\ \zeta_{S_i} = III \\ 13, if\ \zeta_{S_i} = II \\ 15, if\ \zeta_{S_i} = I \end{cases} . \tag{19}$$

6. for the component concerning the efficiency of the change management process in the IT system, it is defined in the following manner: φ_{S_i}

$$\xi_\varphi(\varphi_{S_i}) = 1 + 15 * \left(1 - \frac{\varphi_{S_i}}{100\%}\right). \tag{20}$$

The form of the above-mentioned standardization functions from the family Ξ was defined, for the purpose of the model presented herein, in such a manner so that they transpose their values into appropriate ranges and maintain correct proportions of their impact on the IT system risk.

4. The IT system risk vector

The following vector $\overrightarrow{R_{S_i}}$ is considered the IT system risk model:

$$\overrightarrow{R_{S_i}} = \langle \overrightarrow{R_{S_i}^B}, \overrightarrow{R_{S_i}^C}, \overrightarrow{R_{S_i}^T} \rangle \in M_{m\times n} \times M_{m\times n} \times M_{m\times n} \tag{21}$$

where:

- $M_{m\times n}$ - matrix size: m x n,
- $\overrightarrow{R_{S_i}^B}$ - the vector coordinate $\overrightarrow{R_{S_i}}$ that characterizes an aspect of the IT system security S_i, which constitutes a linear combination of the IT system risk elements S_i within the linear space $(M_{2\times 2}, \boldsymbol{R}, +, \cdot)$.
- $\overrightarrow{R_{S_i}^C}$ - the vector coordinate $\overrightarrow{R_{S_i}}$ that characterizes an aspect of the IT operation business continuity S_i, which constitutes a linear combination of the IT system risk elements S_i within the linear space $(M_{2\times 2}, R, +, \cdot)$.
- $\overrightarrow{R_{S_i}^T}$ - the vector coordinate $\overrightarrow{R_{S_i}}$ that characterizes an aspect of the security of the processes of sensitive data processing in the IT system S_i, , which constitutes a linear combination of the IT system risk elements S_i within the linear space $(M_{2\times 3}, R, +, \cdot)$.

$(M_{m\times n}, R, +, \cdot)$ - Vector space defined as a set of matrices M^{mxn} with an option of adding matrices + external operator· constitutes vector space over the body of real numbers R .
whereas:

$$\overrightarrow{R_{S_i}^B} = \xi_\lambda(\lambda_{S_i}) \cdot \vec{\lambda} + \xi_\alpha(\alpha_{S_i}) \cdot \vec{\alpha} + \xi_\eta^B(\eta_{S_i}^B) \cdot \overrightarrow{\eta^B} + \xi_\beta^B(\beta_{S_i}^B) \cdot \overrightarrow{\beta^B}$$

$$\overrightarrow{R_{S_i}^C} = \xi_\eta^C(\eta_{P_i}^C) \cdot \overrightarrow{\eta^C} + \xi_\beta^C(\beta_{P_i}^C) \cdot \overrightarrow{\beta^C} + \xi_\kappa(\kappa_{P_i}) \cdot \vec{\kappa} + \xi_\pi(\pi_{P_i}) \vec{\pi},$$

$$\overrightarrow{R_{S_i}^T} = \xi_\eta^J(\eta_{P_i}^J) \cdot \overrightarrow{\eta^J} + \xi_\beta^J(\beta_{P_i}^J) \cdot \overrightarrow{\beta^J} + \xi_\delta(\delta_{S_i}) \cdot \vec{\delta} + \xi_\vartheta(\vartheta_{S_i}) \cdot \vec{\vartheta} + \xi_\zeta(\zeta_{S_i}) \cdot \vec{\zeta} + \xi_\varphi(\varphi_{S_i}) \cdot \vec{\varphi}, \tag{22}$$

where: $\vec{\lambda}, \vec{\alpha}, \overrightarrow{\eta^B}, \overrightarrow{\eta^C}, \overrightarrow{\eta^T}, \overrightarrow{\beta^B}, \overrightarrow{\beta^C}, \overrightarrow{\beta^T}, \vec{\kappa}, \vec{\pi}, \vec{\vartheta}, \vec{\zeta}$ - base vectors in the vector space $(M_{m\times n}, \boldsymbol{R}, +, \cdot)$ from algebra $(M_{m\times n}, \boldsymbol{R}, +, \cdot, \otimes)$,
Since the algebra dimension $(M_{2\times 2}, \boldsymbol{R}, +, \cdot, \otimes)$ is (Trajdos, 1993): dim $(M_{2\times 2}, \boldsymbol{R}, +, \cdot, \otimes) = 4$ and $(M_{2\times 3}, \boldsymbol{R}, +, \cdot, \otimes)$: dim $(M_{2\times 3}, \boldsymbol{R}, +, \cdot, \otimes) = 6$, therefore $\left(\overrightarrow{R_{S_i}^B}, \overrightarrow{R_{S_i}^C}, \overrightarrow{R_{S_i}^T}\right)$ 14 base vectors defined in the following way exist to define the components:

$$\vec{\lambda} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}; \ \vec{\alpha} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}; \ \overrightarrow{\eta^B} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}; \ \overrightarrow{\beta^B} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\overrightarrow{\eta^C} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}; \ \overrightarrow{\beta^C} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}; \vec{\kappa} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}; \vec{\pi} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix};$$

$$\overrightarrow{\eta^{C}}=\begin{pmatrix}1&0\\0&0\\0&0\end{pmatrix};\ \overrightarrow{\beta^{C}}=\begin{pmatrix}0&1\\0&0\\0&0\end{pmatrix};\ \vec{\delta}=\begin{pmatrix}0&0\\1&0\\0&0\end{pmatrix};$$

$$\vec{\vartheta}=\begin{pmatrix}0&0\\0&1\\0&0\end{pmatrix};\ \vec{\zeta}=\begin{pmatrix}0&0\\0&0\\1&0\end{pmatrix};\ \vec{\varphi}=\begin{pmatrix}0&0\\0&0\\0&1\end{pmatrix}.$$

On the basis of the above linear combination of such formulas, it is evident that the impact of all of the selected dimensions/factors $\left(\overrightarrow{R_{S_i}^{B}},\ \overrightarrow{R_{S_i}^{C}},\ \overrightarrow{R_{S_i}^{T}}\right)$ of the IT system risk analysis particular risk vector coordinates $\overrightarrow{R_{S_i}}$ is the same. To clarify the estimated IT system risk level, it may be necessary to determine the impact of the particular vector coordinates and risk components on the final IT system risk level as well as to modify such coordinates $\overrightarrow{R_{S_i}}\in M_{\mathrm{m\times n}}\times M_{\mathrm{m\times n}}\times M_{\mathrm{m\times n}}$ by referring to the said impact. This article does not tackle this issue.

5. Magnitude of the IT system risk

Once the IT system risk vector is defined and its coordinates determined according to algebra [20], $(M_{\mathrm{m\times n}}, \boldsymbol{R}, +, , \otimes)$ when we want to determine total risks for the IT system, S_i it is necessary to first set the magnitude $R_{S_i}^{B}$; $R_{S_i}^{C}$; $R_{S_i}^{T}$ and then the value R_{S_i}.

The risk of the IT system $\left(\overrightarrow{R_{S_i}^{B}},\ \overrightarrow{R_{S_i}^{C}},\ \overrightarrow{R_{S_i}^{T}}\right)$ vector $\overrightarrow{R_{S_i}}$ coordinate S_i in algebra $(M_{\mathrm{m\times n}}, \boldsymbol{R}, +, , \otimes)$) is the number $R_{S_i}^{B}$; $R_{S_i}^{C}$; $R_{S_i}^{T}\in\mathcal{R}$ equal to the vector length, i.e.:

$$R_{S_i}^{B}=\left\|\overrightarrow{R_{S_i}^{B}}\right\|\ ;\ R_{S_i}^{C}=\left\|\overrightarrow{R_{S_i}^{C}}\right\|\ ;\ R_{S_i}^{T}=\left\|\overrightarrow{R_{S_i}^{T}}\right\| \quad (26)$$

The presented values $R_{S_i}^{B}$; $R_{S_i}^{C}$; $R_{S_i}^{T}\in\mathcal{R}$ define the magnitude of the IT system risk S_i components in a quantitative manner. To present the risk level, in a qualitative manner, of particular vector coordinates $\overrightarrow{R_{S_i}}$, the following risk ranges may be adopted:

Component $R_{S_i}^{B}$	Component $R_{S_i}^{C}$	Component $R_{S_i}^{T}$
$R_{S_i}^{B}$ *> 70 - catastrophic risk,*	$R_{S_i}^{C}$ *> 70 - catastrophic risk,*	$R_{S_i}^{T}$ *> 70 - catastrophic risk,*
$R_{S_i}^{B}\in(60,\dots,70]$- *very high risk,*	$R_{S_i}^{C}\in(60,\dots,70]$- *very high risk,*	$R_{S_i}^{T}\in(60,\dots,70]$- *very high risk,*
$R_{S_i}^{B}\in(50,\dots,60]$- *high risk,*	$R_{S_i}^{C}\in(50,\dots,60]$- *high risk,*	$R_{S_i}^{T}\in(50,\dots,60]$- *high risk,*
$R_{S_i}^{B}\in(40,\dots,50]$ - *medium risk,*	$R_{S_i}^{C}\in(40,\dots,50]$ - *medium risk,*	$R_{S_i}^{T}\in(40,\dots,50]$ - *medium risk,*
$R_{S_i}^{B}\in(30,\dots,40]$ - *low risk,*	$R_{S_i}^{C}\in(30,\dots,40]$ - *low risk,*	$R_{S_i}^{T}\in(30,\dots,40]$ - *low risk,*
$R_{S_i}^{B}\in(20,\dots,30]$- *very low risk,*	$R_{S_i}^{C}\in(20,\dots,30]$- *very low risk,*	$R_{S_i}^{T}\in(20,\dots,30]$- *very low risk,*
$R_{S_i}^{B}<20$ - *residual risk.*	$R_{S_i}^{C}<20$ - *residual risk.*	$R_{S_i}^{T}<20$ - *residual risk.*

The above-mentioned value ranges were determined on the basis of the practical use of the model presented herein.

The volume of the IT system risks may be defined as the vector module $\left|\overrightarrow{R_{S_i}}\right|$ (Fig. 3):

$$\overrightarrow{R_{S_i}}=\left|\overrightarrow{R_{S_i}}\right|=\sqrt[2]{{R_{S_i}^{B}}^{2}+{R_{S_i}^{C}}^{2}+{R_{S_i}^{T}}^{2}}\ , \quad (23)$$

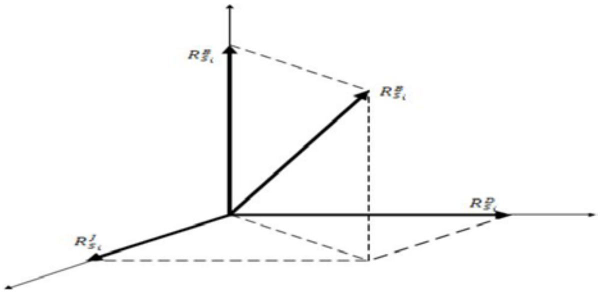

Fig. 3. Vector $\overrightarrow{\boldsymbol{R_{S_i}}}$ of IT system risk in the coordinates configuration $\boldsymbol{R_{S_i}^{B}}$; $\boldsymbol{R_{S_i}^{C}}$; $\boldsymbol{R_{S_i}^{T}}$

6. Evaluation of the IT system risk

Evaluation of the IT system risk consists in the comparison of the results of risk analysis, including the adopted criteria to qualify the risk into the right category (acceptable, tolerable, intolerable risk levels, Fig. 4).

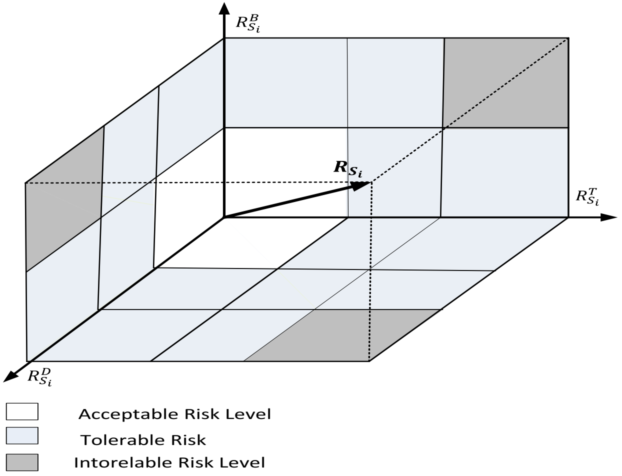

Fig. 4. Map of the IT system risk

The main objective is to provide data that constitute grounds for making a decision on further risk management (whether to process the risk or abandon it, and if the decision is to process the risk - determine to what extent). The risk evaluation process is a summary of the present activities (identification and analysis) and indication which risk or group of risks should be processed further and which may be handled using current control measures.

The risk evaluation has also significant impact on the decision making process. The results of the risk analysis help to decide which risks and to what extent make it necessary for the office to implement a special algorithm for processing such risks and to determine priorities of their processing. The determined risk levels should be then compared with their criteria, including the context agreed at the beginning. In this case, the evaluation shall allow to define the manner of processing a certain risk [21-22].

During the risk assessment process, each risk has to be classified and compared with its tolerable and acceptable level. However, prior to that, it is necessary to adopt certain criteria that would help to explicitly identify significant risks, requiring resolute actions. This is a step in defining the risk that needs special attention. The risk records to be made as a result of the risk assessment shall be helpful in streamlining the risk management process, and hence - crisis management.

Summary

The IT system risk model of the office, described in this article, which includes the process of sensitive data processing, is characterized by high complexity due to the mathematical apparatus applied. Therefore, due to the fact that a number of factors affecting the IT system risk level and its processes were taken into consideration, it is almost impossible to determine the risk of the process of sensitive data processing in terms of time and costs or to manage such risk in a traditional manner, without applying any IT solutions or computer techniques.

Due to a variety of different factors and broad spectrum of their impact on the processes of sensitive data processing, the application of the risk analysis should constitute an integral part of the decision-making process as well as the planning of different variants of the operations of every office unit. The knowledge of the risks associated in the sensitive data processing allows to shape such processes so that their security levels are acceptable (Fig. 4). When analyzing the risk sources and categories in the processes of sensitive data processing, their characteristics, IT system architecture and life cycles should be mainly taken into account. Such knowledge, in combination with the statistics concerning the security and architecture of the system for sensitive data processing, seems to be the key to risk mitigation in all its aspects - human, environmental, security-related, qualitative and economic. The considerations outlined herein are of mainly cognitive importance, thus, formal descriptions of certain issues were omitted. The objective of the article was to show the concept which differs from the traditional view on the issues related to risk quantification.

Bibliography

1. PN-ISO Guide 73:2009, Risk Management – Vocabulary, (2009).
2. R. Hoffmann, M. Kiedrowicz, J. Stanik, MATEC Web of Conferences, *Evaluation of information safety as an element of improving the organization's safety management*, vol. **76**, (2016).
3. R. Hoffmann, M. Kiedrowicz, J. Stanik, MATEC Web of Conferences, *Risk management system as the basic paradigm of the information security management system in an organization*, vol. **76**, (2016).
4. J. Stanik, J. Napiórkowski, R. Hoffmann, *Zarządzanie ryzykiem w systemie zarządzania bezpieczeństwem organizacji*, Zeszyty Naukowe Uniwersytetu Szczecińskiego – Ekonomiczne Problemy Usług, (2016).
5. M. Kiedrowicz, T. Protasowicki, J. Stanik, *Wybrane aspekty standaryzacji w ochronie publicznych zasobów informacyjnych i świadczonych usług w kontekście społeczeństwa informacyjnego*, Zeszyty Naukowe Uniwersytetu Szczecińskiego – Ekonomiczne Problemy Usług, vol. **113**, pp. 113-130, (2014).
6. M. Kiedrowicz, J. Stanik, *Selected aspects of risk management in respect of security of the document lifecycle management system with multiple levels of sensitivity*, (in:) Information Management in Practice, (eds) B.F. Kubiak and J. Maślankowski, pp. 231-249, (2015).
7. M. Kiedrowicz, *Location with the use of the RFID and GPS technologies - opportunities and threats*, GIS ODYSSEY 2016, pp. 122-128, (2016).
8. M. Kiedrowicz, *Objects identification in the information models used by information systems*, GIS ODYSSEY 2016, pp. 129-136, (2016).
9. M. Kiedrowicz, J. Stanik, *Adequacy evaluation of the simulation models of system dynamics on the example of the Earned Value model*, (in:) Information Management (eds) B.F. Kubiak and A. Sieradz, pp. 9-17, (2014).
10. T. Nowicki, M. Marczak, *The modeling analysis and simulation of transport company functioning*. (in:) Modeling of modern enterprises logistics, (eds.) M. Fertsch, K. Grzybowska, A. Stachowiak, (2009).
11. M. Kiedrowicz, Publiczne zasoby informacyjne jako podstawa tworzenia platform integracyjnych, (in:) INTERNET. Prawno-informatyczne problemy sieci, portali i e-usług, (ed.) G. Szpor, pp. 231-246, (2012).
12. M. Kiedrowicz, *Uogólniony model danych w rozproszonych rejestrach ewidencyjnych*, Roczniki Kolegium Analiz Ekonomicznych, vol. 33, pp. 209-234, (2014).
13. M. Kiedrowicz, *Rejestry publiczne wykorzystywane przez organy odpowiedzialne za wykrywanie i przeciwdziałanie przestępczości*, (in:) Rejestry publiczne: Jawność i interoperacyjność, (ed.) A. Gryszczyńska, pp. 603-649, (2016).
14. J. Hash, Risk Management Guidance For Information Technology Systems, ITL Bulletin, National Institute of Standards and Technology, Gaithersburg MD, (2002).
15. J. Stanik, T. Protasowicki, *Metodyka kształtowania ryzyka w cyklu rozwojowym systemu informatycznego*, KKIO „Od procesów do oprogramowania: badania i praktyka”, (2015).
16. M. Kiedrowicz, J. Koszela, *Business processes modelling for the processing of classified documents*

using RFID technology, Collegium of Economic Analysis Annals, vol. **42,** pp. 53-66, (2016).

17. M. Kiedrowicz, J. Koszela, *Secret office model for the processing of classified documents using RFID technology*, Collegium of Economic Analysis Annals, vol. **42,** pp. 67-81, (2016).
18. J. Gołębiewski, *Zarządzanie kryzysowe w świetle wymogów bezpieczeństwa*, pp. 120-121, (2011).
19. M. Kiedrowicz, R. Waszkowski, *Business rules automation standards in business process management systems*, (in:) Information Management in Practice, (eds) B.F. Kubiak and J. Maślankowski, pp. 187-200, (2015).
20. T. Trajdos, Matemetyka, Wydawnictwa Naukowo–Techniczne, (1993).
21. PN-ISO/IEC 27005, Technika informatyczna, Techniki bezpieczeństwa. Zarządzanie ryzykiem w bezpieczeństwie informacji, (2013).
22. PN-ISO 31000:2012, Zarządzanie ryzykiem -- Zasady i wytyczne, (2012).