DOI: 10.1051/matecconf/201712502010

Multi-faceted methodology of the risk analysis and management referring to the IT system supporting the processing of documents at different levels of sensitivity

Maciej KIEDROWICZ[1,*]

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

Abstract. This article outlines the methodology of the IT system risk analysis and management, including various categories of risk factors significant from the point of view of the sensitive data processing and completeness of the procedure for determining the IT system risk level. The presented methodology is divided into the IT system risk analysis and the risk management method. The IT system risk level assessed by the risk analysis method described in this article constitutes an input value for the risk management method outlined in the further part hereof, referring to the IT systems used for the processing of documents at different levels of sensitivity.

Introduction

When analyzing various approaches to assessment of the risk level and proper risk treatment, a question arises whether a possibility of creating a complete and consistent methodology for analyzing the processing of documents at different sensitivity levels, including 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 methodology of the risk assessment and management, referring to the IT system responsible for the processing of the documents at different levels of sensitivity, which is - according to the authors - complete and consistent.

In addition, the provided methodology:

- forms grounds for the qualitative risk assessment and more detailed analysis,
- forms grounds for more detailed methodology of the risk management in the information security process,
- allows risk evaluation[1] at different levels of certainty,
- allows focus on the risk related to the processing of the documents at different levels of sensitivity; it is helpful from the perspective of both the risk resulting "from" (specific risk) and the risk "for" (a given protected value), e.g. fire risk for a certain infrastructure, regardless of the source of such risk,
- allows to apply the scenario approach,
- allows to classify the risks[2] in terms of reliability of the consequence level,
- allows to identify present risks under control and other risks that would require implementation of additional control procedures or enhancement of the present ones,
- delivers results similar to those based on the risk mitigation requirements.

Methodology concept is outlined in Chapter *2. Methodology concept*. Chapter 2.3.4. *Method for calculating the IT system risk* constitutes further elaboration of this concept. Additionally, mathematical formalism allowing to unambiguously determine the risk level of the processing of the documents at different levels of sensitivity also forms a part of the proposed methodology. Such formalism is introduced by subpoints 2.3.4.2.1. - 2.3.4.2.3.

The risk management process should be adapted to the operating organizational structure, clear to everyone and implemented in line with the adopted methodology and law.

In this article, the risk management process is an organized method of risk identification, analysis and evaluation within the framework of the entire risk assessment process, which allows to omit repeatable, rational and efficient risk management activities, as resulting from the risk management strategy.

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

[1] Risk evaluation - process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable [1] definition 3.7.1.

[2] Risk classification - division of risks according to the previously set criteria.

1. Risk elements related to the processing of the documents at different levels of sensitivity

This chapter contains the definition and selected information about the risk and its classification (Chapter 1.1 Definition and classification of risk), with special emphasis on the IT system risks (Chapter 1.2 IT system risks). It also presents certain aspects of ensuring security of the IT systems (Chapter 1.3. Selected aspects of the IT system security), which shall be used in the following part of this document, methodology of the risk analysis and management of the IT system.

1.1. Basic definitions

For the purpose of further consideration, the following definitions have been adopted.
Def. 1. Methodology
Methodology is a set of rules, instructions and good practices intended to outline procedures (methods) in a given situation to attain a goal. It is also presented as a problem-solving approach standardized for a selected area. It is a collection of methods for performing certain activities, achieving certain goals or a set of rules and methods concerning a given action and intention to attain a certain goal. Methodology describes where and how to look for solutions to the problem.
Def. 2. Organization/Office unit - O.
The O-Organization is a deliberately created group of human, capital and ideological resources as well as business activities and information processes interrelated for the purpose of achieving certain goals/objectives of the Office.
Def. 4. set of processes related to the sensitive data processing - P(O).
The organization is also defined as "a set of variable processes with different relationships of interdependence. The organization becomes a space where people integrate around different tasks and problems to be solved. This gives rise to the need to combine various work contents, arrange tasks into processes and create organizational structures according to such processes not according to the authority centers or functional specialization" [2].
The set of the processes related to the sensitive documents processing P is a finite and countable set of processes $P(O) = \{P_1, P_2, \dots, P_i, \dots, P_N\}$, where: N – the number of the processes related to the sensitive documents processing in the *O*-Organization.
Def. 5. Security of sensitive document.
Security of sensitive document - the entirety of actions undertaken to protect data and information processed in the IT or ICT system against unauthorized access, starting from their preparation, through the period of their use and distribution, and ending with their destruction. A sensitive document is considered safe if it has the following properties (security attributes):

- Confidentiality (ISO 27001) - a characteristic that applies to information to ensure that it is not made available or disclosed to unauthorized persons, entities or processes, but only to authorized parties;
- Integrity (ISO 27001) - a characteristic that applies to assets (resources) to ensure their accuracy and completeness; to ensure the accuracy and completeness of information in compliance with its business importance as well as assumptions and methods adopted to process information;
- Availability (ISO 27001) - a characteristic that applies to assets, which are made available and usable upon request of an authorized entity; all these assets and information related thereto must be accessible by authorized entities whenever they need them.
- Authenticity - a characteristic that applies to data to ensure that their origin or content describing an object is in compliance with the declared information;
- Accountability - a characteristic allowing to assign specific actions in the system to a natural person or process and place them in time.
- Non-repudiation - the lack of a possibility to repudiate total or partial participation in the data exchange by one of the participants;
- Reliability (ISO 27001) - a characteristic meaning consistent, intended behavior an effects.

Def. 7. Risk management process. In compliance with the international standards, the risk management process is a process that includes the following activities: risk assessment - inclusive of its identification, analysis and evaluation, decision-making, treatment, monitoring and review. The process refers to all risks and must constitute an integral part of the practical activities of the organization. Additionally, an appropriate party - able to provide correct methods and tools - shall be vested with the execution of such process. The risk management does not only mean preparation of the risk list and actions undertaken with respect thereto. It also requires a serious approach to the risk assessment process, which involves a number of activities, such as risk identification, analysis and evaluation. This is a systematic presentation of the whole undertaking, which requires an appropriately planned strategy.

For the purpose of the methodology described herein, the risk of the sensitive documents processing is defined as a threat, susceptibility or gap (e.g. information, security), since such technologies, i.e. information, design, production, used in a given organization (regardless of its type and scope of business) do not meet the requirements adopted in the organization's strategy or policies, do not provide an appropriate level of quality, security, integrity, availability or continuity of sensitive documents processing, were not properly implemented and do not operate in compliance with the assumptions or requirements of the adopted policies.

With the above in mind, the risk of the sensitive data processing is analyzed in division into various categories [3], sources and areas:

1) possible sources of risk: natural and technical risks, deficient (lack of) legislation, inappropriate habits, human mentality, weakness of the organization, lack of training, low awareness of

risks, lack of readiness, unprepared personnel, lack of system, unrealistic security standards, quality standards, continuity of operations standards, technical and technological delays, non-compliance with technological norms, operational errors, negligence and omissions, ignorance, incompetence, (system) corruption,

2) possible risk areas: organization, organizational unit, department, natural environment, communities, business processes, security environment, information processes, etc.

1.2. Documents at different levels of sensitivity

The documents at different levels of sensitivity include such documents that require special approach to their management. They may contain confidential information as well as data that need to be specially protected due to other reasons (e.g. banking documents). The aforesaid documents are usually handled in dedicated rooms specially adapted for that purpose - therefore, such terms as "secret office or "RFID office"[3] shall be also used further on in this article. The main objective of this article is to outline major aspects of the organization and functioning of the offices responsible for the processing of confidential documents and materials, in compliance with the effective legislation in Poland, as well as the methodology of risk management with respect to the office processes, where the basic functionality is supported by implementation of the dedicated IT systems and technologies, e.g. RFID [4-6. 32- 34, 38].

The processing of documents at different levels of sensitivity by the office is based on current legislation, which defines basic activities, resources and participations of such activities. The office is the key subject of the above-mentioned process. Every office performs many activities related to the processing of various documents. As far as the secret office (SO) is concerned, the processed documents are at different levels of security classification. The acts and resolutions, which constitute basic analytical and research resources, are among the most important publications.

While developing the methodology of risk management with respect to the office responsible for the processing of classified documents and processes, and outlying the rules and methods of operations of such unit, the national legislation needs to be taken into account.

The term "sensitive document" was not legally defined on the basis of the binding provisions of law. The common language only knows the term "sensitive data", which mainly refers to personal data. Therefore, the article tackles the idea of the documents which contain some confidential information, intended not for an unlimited, but a narrow group of recipients, due to the nature and potential damages that may occur if such information is disclosed.

1.3. Risk related to sensitive documents

A special type of risk discussed herein is the risk related to sensitive documents, which also has not been defined in an explicit manner. For the purpose of IT advisory and methodology presented in the article, the risk of sensitive documents defined as a threat that the IT technology or other technologies applied in a given office unit (regardless of its type and scope of business):

– have not been properly implemented and do not work in line with their assumptions,
– prevent implementation and upgrade of technical and technological infrastructure supporting the risk management process, in accordance with the present risk profile,
– do not ensure sufficient security of the Office and its resources at an acceptable level,
– do not meet the requirements included in the following policies: security policy, quality policy, business continuity management policy, etc.,
– do not provide appropriate organization structure in terms of security services,
– do not ensure appropriate maintenance of the relevant documentation concerning security, quality or continuity of operations,
– do not ensure proper integrity, confidentiality, non-repudiation and access to sensitive data.

In light of the above, the risk of sensitive documents is analyzed in division into the following categories and attributes:

1) the following attributes in the field of information security: access to sensitive documents, confidentiality of the processed data, integrity of documents, fulfillment of security requirements included in the security policy, losses understood as a costs incurred due to the loss of security attributes [7,8,35-37];
2) the following elements in the field as resulting from the legal norms regulating such security issues: appointment of a representative to protect classified information, creation of a security division in the organization to perform tasks related to the processing of sensitive documents in the organization, adaptation of the office facilities to the requirements on creation, processing, acceptance, assignment, delivery and protection of sensitive documents according to the provisions of law; organization of a secret office, organization of a special location (place, facility) for the processing of sensitive data, including ICT systems for executing and processing sensitive documents;
3) the following documents in the field of basic quality and security documents: risk analysis reports, security policy, ICT security plan, special security requirements for the ICT system, safe use procedures and business continuity plan;

[3] RFID (radio-frequency identification) – a technique that uses radio frequency to send data and supply the electrical system (RFID tag), which constitutes track tags attached to objects for the purpose of their identification. It allows reading and sometimes also recording the RFID system. Depending on its structure, the technology allows to read tags from the distance of several dozen centimeters or several meters from the reader antenna.

4) the following attributes/measures in the field of the sensitive information security processing process: importance of the Office and its Clients, fulfillment of the requirements included in the quality policy;
5) the following attributes in the field of security of business continuity: fulfillment of the requirements included in the business continuity management policy, financial effects of suspension/interruption of the process, non-financial effects of suspension/interruption of the process, costs and time of the process unavailability;
6) In other fields: flexibility of the process of sensitive data processing, costs and time of the process of sensitive data processing, efficiency of the change management process, efficiency of the management process architecture related to the processing of sensitive data, reliability.

Last but not least, it should be stressed that the risk of sensitive documents may result from such an allegedly prosaic reason as wrongly designed user interface in the ICT system.

Therefore, it is evident that risks may not be completely eliminated from the organization. However, there are methods of risk assessment, in particular with respect to the risk related to the processing of documents at different levels of security, and methods of risk mitigation, which are described in the following part hereof.

2. Concept of the risk analysis and risk management methodology referring to the IT system supporting the processing of sensitive data

2.1. Assumptions

The methodology proposed herein constitutes a comprehensive approach to the risk analysis and management related to the processing of documents at different levels of sensitivity, including different categories of factors, whose impact on the risk is described in *Chapter 1. Risk elements related to the processing of the documents at different levels of sensitivity.* The risk of sensitive documents and security elements are often neglected in the current risk analysis approaches, which - according to the author - are characterized by significant impact on the total risk of sensitive documents.

The methodology presented in the article takes into consideration all of the sensitive documents in the organization, therefore, there is no phase of selecting the processes of sensitive documents to be included in the risk analysis and later risk management procedures. The above approach allows comprehensive and relatively objective analysis of the processing of the documents at different levels of sensitivity within the organization. Apparently, there is no reason not apply the proposed methodology in case of the selected processes related to the processing of the document at different levels of sensitivity. Additionally, the methodology described herein assumes that each change in the process of sensitive data processing that changes the risk levels has impact only on such process and does not affect any other processes related to the processing of the documents at different sensitivity levels. On the basis of such assumption, it is evident that one vector of change of the process risk may affect only one process of the processing of sensitive data.

2.2. Methodology concept

The general scheme of the proposed methodology is outlined in Fig. 1. The described methodology is composed of the following elements [7, 8]:

– The principles of risk management [3], whose comprehensive implementation within the entire office (e.g. Secret Office) and particular areas of its operations, may be translated into the risk management efficiency.
– Risk management framework [4] – a set of components that ensure foundations and organizational arrangements in terms of design, implementation, monitoring, review and improvement of the risk management process within an organization.
– Risk management process[5] - the process that falls within the scope of responsibilities of the management and personnel of an organizational unit, designated to identify risks and compare action strategies of the organization, which may have positive or negative impact on the functioning of the organization and - while considering achievement of the specific objectives - protection of the organization against the risk above its acceptable level[6]. The risk management process also refers to

[4] [1] definition 2.1.1.

[5] In compliance with the international standards, the risk management process is a process that includes the following activities: risk assessment - inclusive of its identification, analysis and evaluation, decision-making, treatment, monitoring and review. The process refers to all risks and must constitute an integral part of the practical activities of the organization. Additionally, an appropriate party - able to provide correct methods and tools - shall be vested with the execution of such process.

[6] Acceptable risk - the risk magnitude that may be accepted by the organization, without any additional remedial actions or changes in the operations. Acceptable risk level - a conventional value. It is the result of the risk assessment process, which includes a comparison of the risk level defined during an analysis with the adopted criteria. It is determined whether the expected risk falls within the limits of acceptance and tolerance or not. Each risk, whose value goes beyond the acceptable level, but falls within the tolerance limits, should increase vigilance and initiate actions aimed at monitoring, controlling and mitigating such risk. However, before undertaking any actions, it is essential to evaluate efficiency of the monitoring process, reliability of the information, correctness of the analysis, possible losses or advantages of risks, expected expenses related to the risk mitigation and cost effectiveness of the whole undertaking [9].

the reduction of uncertainties and possibilities of dealing therewith.

- Method of the IT system risk analysis and the risk management method.

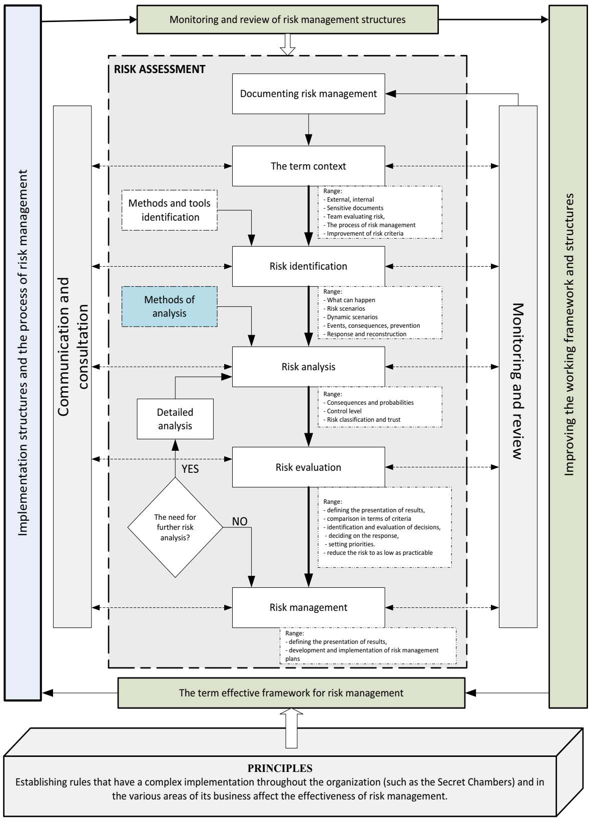
Monitoring and review of risk management structures
RISK ASSESSMENT
Documenting risk management
The term context
Range:
- External, internal
- Sensitive documents
- Team evaluating risk,
- The process of risk management
- Improvement of risk criteria
Methods and tools identification
Risk identification
Range:
- What can happen
- Risk scenarios
- Dynamic scenarios
- Events, consequences, prevention
- Response and reconstruction
Methods of analysis
Risk analysis
Range:
- Consequences and probabilities
- Control level
- Risk classification and trust
Detailed analysis
YES
Risk evaluation
The need for further risk analysis?
NO
Range:
- defining the presentation of results,
- comparison in terms of criteria
- identification and evaluation of decisions,
- deciding on the response,
- setting priorities.
- reduce the risk to as low as practicable
Risk management
Range:
- defining the presentation of results,
- development and implementation of risk management plans
Implementation structures and the process of risk management
Communication and consultation
Monitoring and review
Improving the working framework and structures
The term effective framework for risk management
PRINCIPLES
Establishing rules that have a complex implementation throughout the organization (such as the Secret Chambers) and in the various areas of its business affect the effectiveness of risk management.

Fig. 1. Concept of the methodology of risk analysis related to the processing of the documents at different levels of sensitivity.

Taking into account the assumptions and limited number of pages of particular articles in this study, only general characteristics of individual stages of the risk management process and the method of risk assessment was presented further on herein, with respect to every process of the processing of documents at different levels of sensitivity. Special emphasis was placed, in this methodology, on the definition of the manner of presenting the risk assessment results in the form of the risk vector of the processing of the documents at different levels of sensitivity – *Chapter 2.3.4.*

2.3. Risk management process

The process includes five main tasks: communication and consultation[7], context determination, risk assessment[8], risk treatment, monitoring and review.

2.3.1. Communication and consultation

The principles of communication and consultation shall be determined before implementing subsequent elements of the process. Such activities should consider not only the issue of the risk as such (including its causes and consequences), but also the stage of the risk treatment. It is important, since this element constitutes grounds for proper communication with all involved parties and entities in the organization and its interested parties. Communication and consultation are not the goals as such - what is really important is their proper use allowing to understand the decisions being made and their expected consequences.

2.3.2. Establishing context

None of the organizations functions in empty space, therefore it is crucial to analyze external and internal correlations as well as their impact on the risk and the risk management process. While the external correlations not always depend on the organization, the internal correlations may, should and must be subject to rational approach to risk management. Therefore, it is essential to determine the context[9]. When determining the context of the risk management process, special attention should be paid to the fact that this process must refer to the defined objectives, responsibilities as well as the scope and scale of the undertaken actions. It is also essential to include the adopted method of risk assessment, ways of evaluating its results and criteria. What is more, agreement on the risk criteria constitutes an important element of such process. Above all, it allows to determine its materiality by referring to the values of the organization as well as its targets and missions. The standard shows that by determining the aforesaid criteria, the following should be taken into account[10]:

1) nature and types of causes and consequences, which may occur, and the manner of their measurement,
2) manner of defining the probability of their occurrence,
3) timeframe of the occurrence probability and/or their consequences,
4) manner of establishing the risk level,
5) acceptable or tolerable risk level.

It is necessary to answer the question whether the organization shall analyze every risk separately or in groups (after determining which correlations of such groups need to be examined). It is equally important to secure the whole process in terms of: information, personal, financial, logistic and technical data. The risk management process should be adapted to the operating organizational structure, clear to everyone and implemented in line with the adopted methodology and law. Competence and responsibility of the personnel should be precisely divided, whereas the risk criteria clearly defined and in compliance with the organization's targets.

[7] Communication and consultation - continuous and iterative processes, which are carried out by the organization to ensure, provide or obtain information as well as to communicate with the interested parties as regards risk management, [1] definition 3.3.1.2.

[8] Risk assessment - the entire process of risk assessment, Risk analyses and risk evaluation, [1] definition 3.4.1., cf.: [10]

[9] cf.: [3] pp. 43-47.

[10] [3], p. 47.

2.3.3. Risk assessment

Another important action is the risk assessment process. It requires the preparation of an exhaustive list of risks[11]. Risk assessment may be performed in three stages:

- Definition of sensitive resources.
- Identification of susceptibility and risks of such resources.
- Risk measurement.

When defining sensitive resources, it is important to make a list of information objects or information processing processes, which require protection on the basis of an appropriate catalog of resources and common sense. The process requires knowledge of law and full understanding of the operational mechanism in the organization [7, 11, 29-31].

The aim of risk assessment is to create the broadest possible list of risk factors, which may have impact on the defined sensitive resources - regardless of whether their sources are under the control of the office unit or not. When identifying the risk, the cascading effect (Domino)[12], which stimulates the occurrence of further risks[13], needs to be taken into account.

The point of risk identification is to prepare the full list of risk factors, resulting from potential events that - depending on the circumstances - may create, prevent, limit, accelerate, delay or make it impossible to achieve a goal.

Risk identification is a continuous process, as the risks or risk factors not detected on time may not only make it impossible to achieve the goal, but also pose threat to the organization. The basis for such risk identification shall be the information that needs to satisfy certain criteria. It should be reliable, prompt, complete and - if possible - verified. Therefore, there are several requirements for the information sources and people responsible for such tasks. The sources must be reliable and safe, whereas the people well prepared. The risk components are the following:

1) sources of risks or threats,
2) events or incidents being the risk sources,
3) consequences for the organization and environment,
4) causes of current threats or occurring events,
5) efficiency of the monitoring and detection systems,
6) place and time of risk occurrence.

The aforesaid components shall be analyzed separately with respect to every event that may pose threat (hurricanes, floods, legislative risks, etc.).

1. *Possible identification methods: measurements*, discussions, experiences, expert opinions, laboratory tests, detection systems, modeling, scenarios, questionnaires, forecasts, risk analyses, structures, solutions (weaknesses and strengths, possibilities and needs).
2. *Possible sources of risk:* natural and technical risks, deficient (lack of) legislation, inappropriate habits, human mentality, weakness of the organization, lack of training, low awareness of risks, lack of readiness, unprepared personnel, lack of system, technical and technological delays, non-compliance with technological standards, operational errors, negligence and omissions, ignorance, incompetence, (system) corruption.
3. *Possible risk areas:*[14]: organizational unit, department, natural environment, development processes, security environment, information processes, etc.

Subsequently, the aggregated risk[15] needs to be analyzed. The point of risk analysis is to allow detailed understanding thereof. The knowledge gained at this stage allows to make a decision on the method of risk treatment (choice of the strategy[16] and selection of methods)[17]. The analysis should be aimed at determining potential consequences of risks and probability of their occurrence (the following data may be found as results: qualitative, semi-quantitative, quantitative or a combination thereof, depending on the needs of the organization and selected method).

2.3.4. Method of the IT system risk measurement.

2.3.4.1. Assumptions

The widely applied methods of efficient risk assessment are risk maps or matrices. They are composed of two combined (usually five step) scales: probability and consequences, allowing to define the acceptance level of a given risk.

[11] In compliance with [1], the risks are considered sources of potential damages, whereas the risk is expressed with reference to potential consequences and probability of their occurrence.

[12] Domino effect - a theory assuming that one event sets off a chain of events.

[13] This element is important, since some risks (threats) may occur only as consequences of other risks.

[14] Risk area - the area of risk factors, which are significant from the point of view of a given entity.

[15] Risk aggregation - description of a set of risks.

[16] Strategy of risk treatment - theory and practice aimed at implementing the assumed long-term targets under the risk modification process.

[17] Method of risk treatment - a way of modifying the risk, including, among other things, avoiding the risk, taking or increasing the risk, removing the risk source, changing the consequences, division of risk, risk retention. Source: own elaboration based on [1] definition 3.8.1

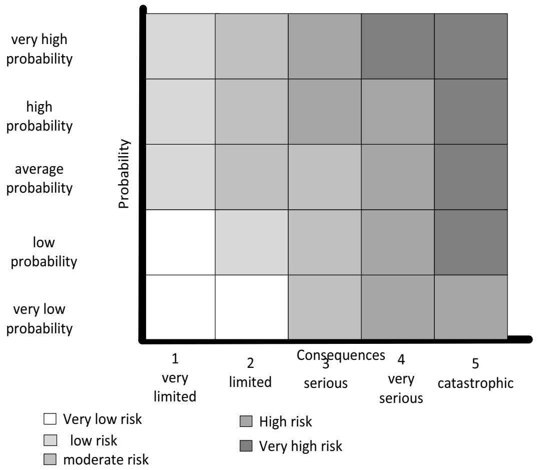

Fig.2. Risk matrix example.

The risk matrix shows that the risk is assessed on the basis of only two basic components, i.e. probability and consequences. In this approach other components/risk factors, described in Chapter 1 hereof, which include security, quality and business continuity parameters, are insignificant. With the above in mind, it seems justified to assess the IT risks by using the vector which $\overrightarrow{R_{S_i}}$ reflects the IT system risk levels in its all possible aspects. On the other hand, each considered aspect/area should specify all basic risk factors (threats, susceptibility and security mechanisms). For example, when considering the area of information security, the security of areas referring to sensitive data processing and business continuity of the IT system risk vector may be defined in the following way:

$$\overrightarrow{R_{S_i}} = \left(\overrightarrow{R_{S_i}^{B}}, \qquad \overrightarrow{R_{S_i}^{C}}, \qquad \overrightarrow{R_{S_i}^{T}}\right)$$

where:

- $\overrightarrow{R_{S_i}^{B}}$ - the vector coordinate $\overrightarrow{R_{S_i}}$ that characterizes an aspect of the IT system information security S_i,
- $\overrightarrow{R_{S_i}^{C}}$ - the vector coordinate $\overrightarrow{R_{S_i}}$ that characterizes an aspect of the IT system continuity of operations 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 process of sensitive data processing in the IT system S_i,.

The selected coordinates of the risk vector represent individual risk areas (Fig. 3), each of them including several risk factors, hereinafter referred to as the composition of partial vectors of IT system risk.

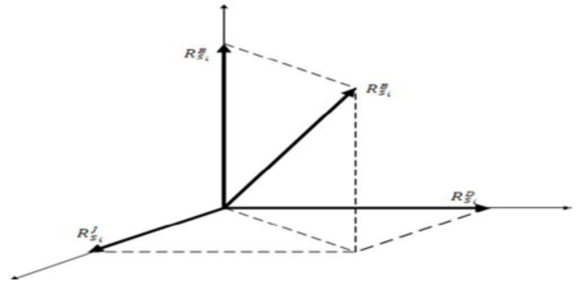

Fig. 3. Vector $\boldsymbol{R_{S_i}^{B}}$ of IT system risk in the coordinates configuration $\boldsymbol{R_{S_i}^{B}}$; $\boldsymbol{R_{S_i}^{D}}$; $\boldsymbol{R_{S_i}^{T}}$

Its visualization in the form of a "risk cube" is shown in (Fig. 4.)

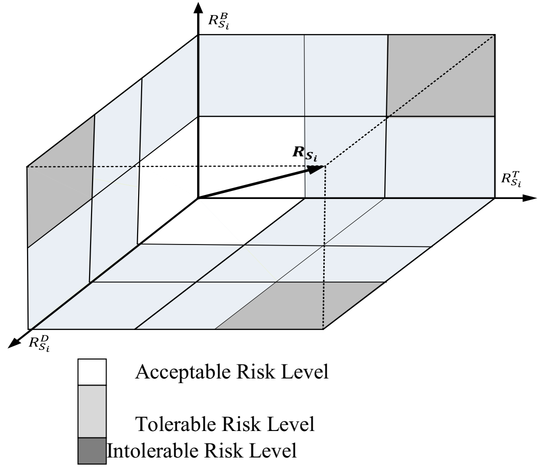

Fig.4. Risk cube of the IT system.

The method of IT system risk measurement should be also applied in such a manner so that it provides sufficient input data for risk evaluation.

2.3.4.2. Review of the procedure

The IT system risk assessment is performed in the following steps. General scheme is shown in Fig. 5.

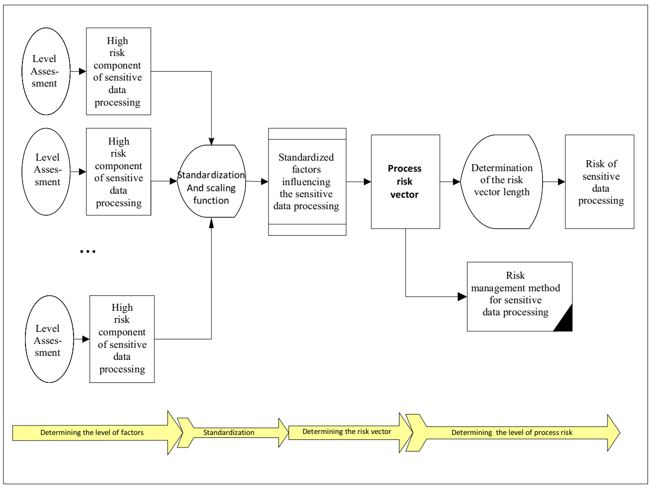
Level Asses-sment
High risk component of sensitive data processing
Level Asses-sment
High risk component of sensitive data processing
...
Level Asses-sment
High risk component of sensitive data processing
Standardization And scaling function
Standardized factors influencing the sensitive data processing
Process risk vector
Determination of the risk vector length
Risk of sensitive data processing
Risk management method for sensitive data processing
Determining the level of factors
Standardization
Determining the risk vector
Determining the level of process risk

Fig. 5. General scheme of the risk assessment processes referring to the processing of the documents at different levels of sensitivity.

1) Definition of risk factors affecting the risk. The method includes several factors that, according to the author, allow a relatively objective and accurate assessment of the risk level related to the processing of the documents at different levels of sensitivity. Different elements of the risk analysis used in the methodology described herein are presented in Chapter *1.* The level of detail referring to the selected components is determined by the correlations between the risk analysis and architecture of the processes related to the processing of the documents at different levels of sensitivity.
2) Standardization of the defined factors having impact on the risk.
3) Determination of risk vector based on the standardized values of the risk components.
4) Determination of impact weights of particular factors on the total risk level for a given IT system. Such impact weights are determined depending on the confidentiality clause - the level of sensitivity, at which a given organizational unit operates.
5) Determination of the weighted risk vector. The vector includes impact of the level of the document sensitivity, at which a given organizational unit operates, on the processing process risk.
6) Determination of the final risk level referring to the processing of the documents at different levels of sensitivity. Method of risk assessment is described in Chapter*2.6.*

2.3.4.2.1. Standardization

Due to the fact that the components of the IT system risk and processes of the sensitive data processing, as a matter of principle, belong to different sets of values, it is necessary to introduce a function or a set of functions clearly transferring such components to a uniform range of values [1,..., *N*]. The adoption of such range of values [1,..., *N*] is aimed at creating the simplest possible shape of the functions that would transpose the components of the described model into a uniform range of values, additionally ensuring legibility of the risk analysis results. The exclusion of this range of values lower than 1, in particular 0 values, from such range is associated with the concept of a residual risk, [12], according to which it is impossible to completely eliminate the risk, thus, none of its components presented in the method of analysis of the process risk may have zero value. To transpose the values of the individual components of the risk of the processes of sensitive data processing into the uniform range of values, we have introduced the concept of the standardization function. The standardization function is a family of functions $\xi\colon X \longrightarrow [1, 2, \dots, N]$ determined for the selected components of the business process risk.

For example, in case of the component related to the confidentiality of data processed in this process - $\boldsymbol{\alpha_{P_i}}$ function ξ_α can be defined as follows:

$$\xi_\alpha\left(\alpha_{P_i}\right) = \begin{cases} 1, if\ \alpha_{P_i} = F \\ 2, if\ \alpha_{P_i} = E \\ 3, if\ \alpha_{P_i} = D \\ 4, if\ \alpha_{P_i} = C \\ 6, if\ \alpha_{P_i} = B \\ 8, if\ \alpha_{P_i} = A \end{cases}; \qquad (1)$$

$where$:
$P_i \epsilon P(O),\ \ \xi_\alpha \epsilon \Xi],\ \alpha \epsilon \mathrm{A}$ – set of confidentiality classes.

The forms of the standardization function from the family Ξ should be defined in such a manner so as to transpose their values to the range [1,..., N] and keep the right proportions of their impact on the risk of the process of sensitive data processing. Another limitation is to express the M number of the selected standardization function from the family Ξ as a product of two natural numbers larger than 1, i.e.: $\|\Xi\| = M = m \times n,\ m > 1, n > 1$. Furthermore, the point is to obtain a product $M \times N \cong 100$ - then a calculated length of the risk vector of the process of sensitive data processing could be measured in percentage and easily interpreted.

2.3.4.2.2. Risk vector of particular components of the IT system

Once the vector space is defined $(M_{\mathrm{m}\times\mathrm{n}}, \boldsymbol{R}, +,\cdot)$ in algebra, $(M_{\mathrm{m}\times\mathrm{n}}, \boldsymbol{R}, +,\cdot,\otimes)$ it is possible to introduce the concept of the risk vector for each coordinate of the IT system risk vector.

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

$$R^B_{S_i} = \left\|\overrightarrow{R^B_{S_i}}\right\|\ ;\ R^D_{S_i} = \left\|\overrightarrow{R^D_{S_i}}\right\|\ ;\ R^T_{S_i} = \left\|\overrightarrow{R^T_{S_i}}\right\| \qquad (2)$$

whereas: The risk vector of any coordinate $\left(\overrightarrow{R^B_{S_i}},\ \overrightarrow{R^C_{S_i}},\ \overrightarrow{R^T_{S_i}}\right)$ in algebra $(M_{\mathrm{m}\times\mathrm{n}}, \boldsymbol{R}, +,\cdot,\otimes)$ is the vector $\overrightarrow{R^X_{S_i}} \in M^{mxn}$; gdzie X ∈ {B, C, T} being a linear combination of the system risk elements S_i in the linear space$(M_{\mathrm{m}\times\mathrm{n}}, \boldsymbol{R}, +,\cdot)$:

$$\overrightarrow{R^X_{S_i}} = \xi_{\alpha^1}\left(\alpha^1_{P_i}\right) \cdot\overrightarrow{\alpha^1} + \xi_{\alpha^2}\left(\alpha^2_{P_i}\right) \cdot\overrightarrow{\alpha^2} + \cdots + \xi_{\alpha^M}\left(\alpha^M_{P_i}\right) \cdot\overrightarrow{\alpha^M}$$

Algebra dimension $(M_{\mathrm{m}\times\mathrm{n}}, \boldsymbol{R}, +,\cdot,\otimes)$ [13] is: dim $(M_{\mathrm{m}\times\mathrm{n}}, \boldsymbol{R}, +,\cdot,\otimes) = M$.
Due to the fact that the algebra dimension $(M_{\mathrm{m}\times\mathrm{n}}, \boldsymbol{R}, +,,\otimes)$ is *N*, it is evident that *N* of base vectors in the vector space does exist $(M_{\mathrm{m}\times\mathrm{n}}, \boldsymbol{R}, +,\cdot)$ from algebra $(M_{\mathrm{m}\times\mathrm{n}}, \boldsymbol{R}, +,,\otimes)$, defined in the following manner:

$$\overrightarrow{\alpha^1} = \begin{pmatrix} 1 & \cdots & 0^n \\ \vdots & \ddots & \vdots \\ 0^m & \cdots & 0^M \end{pmatrix}; \dots ; \overrightarrow{\alpha^M} = \begin{pmatrix} 0 & \cdots & 0^n \\ \vdots & \ddots & \vdots \\ 0^m & \cdots & 1 \end{pmatrix} \qquad (3)$$

On the basis of the above linear combination of such formula, it is evident that the impact of all M of the selected risk analysis factors on the obtained coordinate

$\overrightarrow{R_{S_i}^X}$ of risk vector $\overrightarrow{R_{P_i}} \in M^{mxn}$ is the same. Therefore, 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 $\overrightarrow{R_{S_i}^X} \in M^{mxn}$ by referring to such impact weights. This article does not tackle this issue.

2.3.4.2.3. Determination of the final IT system risk level

Once the values have been set $R_{S_i}^B$; $R_{S_i}^D$; $R_{S_i}^T \in \mathcal{R}$, which define in a quantitative manner the volume of the IT system risk impact S_i. it is possible to determine the final IT system risk level. The magnitude of the IT system risks may be defined as the vector module $\left|\overrightarrow{R_{S_i}}\right|$:

$$\overrightarrow{R_{S_i}} = \left|\overrightarrow{R_{S_i}}\right| = \sqrt[2]{{R_{S_i}^B}^2 + {R_{S_i}^D}^2 + {R_{S_i}^T}^2} \ ,$$

The presented value R_{S_i} defines in a qualitative manner the magnitude of the IT system risk impact P_i, which constitutes the final value of the method of the IT system risk analysis described herein. To present the risk level in a qualitative manner, determined by the above-mentioned qualitative method, the following risk ranges may be adopted: $R_{P_i}> 70$ – catastrophic risk, $R_{P_i} \in (60, \dots, 70]$ – very high risk, $R_{P_i} \in (50, \dots, 60]$ – high risk, $R_{P_i} \in (40, \dots, 50]$ – medium risk, $R_{P_i} \in (30, \dots, 40]$ – low risk, $R_{P_i} \in (20, \dots, 30]$ – very low risk, $R_{P_i} < 20$ – residual risk.

2.3.5. Risk evaluation

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).

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 [14-15].

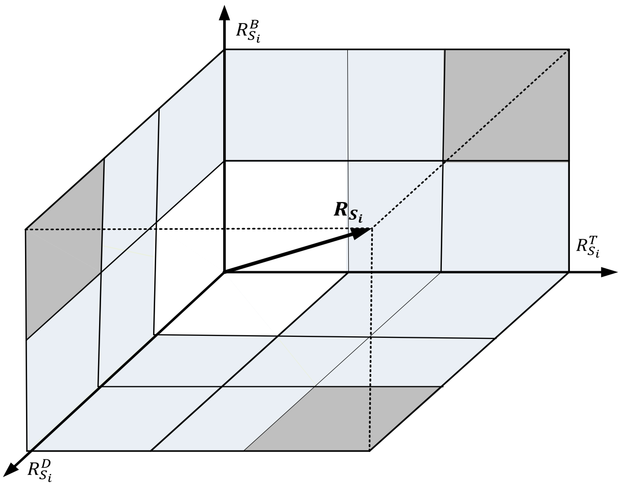

Fig. 6. Map of the IT system risk.

□ Acceptable Risk Level

▨ Tolerable Risk Level

■ Intolerable Risk Level

Risk evaluation, as the last step in the risk assessment process, includes a comparison of the risk level identified during an analysis with the adopted criteria. Such comparison requires great accuracy and reliability. It is determined whether the expected risk falls within the limits of acceptance and tolerance or not. The accepted risk does not require any special attention (daily activities), whereas the risk within the tolerable limits should increase vigilance and initiate actions aimed at its monitoring, control and mitigation mechanisms. Risk tolerance does not mean acceptance of the status quo, it requires a response. However, before undertaking any actions, it is essential to evaluate efficiency of the monitoring process, reliability of the information, competency of staff, correctness of the analysis, possible losses or advantages of risks, expected expenses related to the risk mitigation and cost effectiveness of the whole undertaking. The higher the risk level, the more attention needs to be paid - preparation of special programs that may be implemented to eliminate or mitigate such risks, execution of a relevant process and scope of activities brining the risk to the tolerance or acceptance level, depending on the necessity of counteracting the costs of the effects and expenses regarding the adopted criteria. Such criteria should result from the organization's readiness, however the organization's ability to handle the risks depends on its personnel and parameters: size, structure, equipment, financial possibilities, professional approach as well as sensitivity and resistance to the expected risk. The main condition is to focus on bringing the risk to acceptable level. It is not always possible - in certain circumstances, some factors justifying the risk tolerance above its acceptable level may occur. The said circumstances may be the following:

1) the organization's possibilities go beyond its needs in terms of managing some acceptable risks, thus, it may be allowed, from time to time, to increase the risks for the purpose of benefiting from the

circumstances that may constitute an opportunity for the organization,
2) the risk level beyond the acceptable limits is so low that it does not require any special treatment or programs within the framework of the available resources,
3) the risk is not specified and does not fall within the organization's monitoring process,
4) the costs of risk management and mitigation, including the insurance and security costs, are disproportionate to potential profits; the only option would be to tolerate the risk that only slightly exceeds the acceptance limits.

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.

2.3.6. Risk treatment

The starting point in risk management is composed of two levels: the first one - not requiring any other procedure than the monitoring process, always acceptable, and the second one - not tolerable, requiring immediate remedies aimed at brining the risks to the tolerance zone. The risk falling between those two levels shall be assessed in economic terms (costs and profits), e.g. in the management process related to residual risk. Nonetheless, the risk is not constant and may escalate towards non-tolerable level. Such risk requires more attention and needs to be monitored. Therefore, it is justified to qualify the risk as "non-tolerable". The actions need to be taken immediately, when the estimated cost/effect comparison is < 1. The risk within such range is considered reasonably practical, but needs to be monitored and the organization needs to prepare itself for appropriate reaction when the said circumstances appear. Such preparation shall include:

1) determination of the absolute scale of the expected risk,
2) broadening of knowledge, improvement of methods and arrangements related to the risk reduction or modification and its consequences,
3) ensuring appropriate readiness level to face the situations, when undesired events may occur due to the risk escalation,
4) readiness to incur any costs of potential losses, if the actions aimed at eliminating or mitigating the risks and preventing undesired events caused thereby or threats resulting therefrom proved inefficient.

Risk assessment determined the method of risk treatment. Such methods are defined in the following standard[18]:

1) avoidance of risk by making decisions on non-commencement or discontinuance 2. decrease or increase of risk to benefit from an opportunity,
2) elimination of the risk source,
3) change of probability (of risk occurrence),
4) change of consequence,
5) sharing of risk with another party or parties (including contracts and risk financing),
6) keeping the risk based on a conscious decision. To choose the right method of risk treatment, it is essential to consider all costs in terms of potential profits. However, it is not a prerequisite. According to the standard, it is recommended to include also such risks that are hard to justify, while considering only the cost effectiveness of the choice. The so-called severe risks (with high negative consequences, but low probability) should also be analyzed.

The method of risk treatment should also be articulated and properly described. The risk treatment plans are used for that purpose. They should include the majority of the previously indicated elements, i.e.[19]:

1) justified choice of a given treatment option,
2) persons responsible for its implementation,
3) proposed actions,
4) requirements concerning the resources, including those for crisis preparedness,
5) reporting and monitoring requirements,
6) time framework and schedule.

2.3.7. Monitoring and review

The last two actions are monitoring and review. The monitoring process should be included already at the plan preparation stage (periodic), even though - according to the standard - the process should be also verified ad hoc. While developing the plans, it is essential to explicitly assign responsibility for this action and include all aspects of risk management therein. The monitoring process is aimed at tracking all changes occurring in the environment, not eliminating or mitigating the risk, but providing information thereon. It also constitutes grounds for performing actions and controlling the risk. Only permanent monitoring may contribute to confidence in information. Everything is subject to change: environment, atmosphere, sensitivity, organizations, law, programs and processes. Such changes affect targets, rules, policies and risk management practices. The monitoring and review processes should be also properly documented. The point is to not only document the processes, but also, or even above all, to create appropriate conditions for improvement and refinement of the selected methods and tools. Apart from the International Standard Organization (ISO), there are also several other recommendations concerning risk management, such as the British standard published by the Federation of European Risk Management Associations (FERMA) or American Enterprise Risk Management – Integrated Framework, known as COSO_II, which was developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

[18] [3], p. 51.

[19] [3], p. 53.

All these norms and standards, similarly to those mentioned at the beginning hereof, are based on similar assumptions. The goal is to define links between the organization's targets, including all risk management elements, i.e. context determination, risk assessment, risk response and treatment, control actions, information and communication principles, as well as monitoring through constant evaluation of the obtained results [16-21].

2.4. Documentation of risk management

The documented[20] actions related to risk management constitute one of the last elements of the pillar related to the above-described processes. According to the standard, it is also recommended to use the available tools for consolidating the knowledge of identified risks as well as actions and decisions made during the risk management process. This element fulfills several important functions, thanks to which the organization is able to accomplish its goals. Therefore, it is even more important to be able to learn and improve internal methods and processes implemented under the risk management procedure. The documentation of data also brings some benefits in terms of management of the organization, by supporting its decision-making process thanks to a possibility of multiple use of the archived historic sensitive documents [22, 23, 5, 6, 24, 39]. The guidelines on risk documentation, applied in office units, point to at least two types of the used documents. The first type refers to identification worksheets or risk identification and assessment worksheets. They are used as basic material for risk analysis. The second type of the documents are the so-called risk registers[21]. They include extended information on the identified and assessed risks, including defined actions to be taken with respect thereto. The risk registers most often constitute integrated lists enclosed with risk reports, which are subject to verification and analysis at the stage of monitoring and review [11, 25-27].

Summary

The methodology of the risk analysis and management referring to the IT system supporting the processing of documents at different levels of sensitivity, is characterized by high complexity due to the mathematical apparatus applied. Therefore, due to the fact that a number of factors affecting processes risk level 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 each organization. The knowledge of the risks associated in the sensitive data processing allows to shape such processes so that their security levels are acceptable [4, 28]. When analyzing the risk sources and categories in the processes of sensitive data processing, their characteristics, process architecture and its life cycle should be mainly taken into account. Such knowledge, in combination with the quality statistics concerning the security and architecture of the process 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.

References

1. PN-ISO Guide 73:2009, Risk Management – Vocabulary, (2009).
2. C. Sikorski, *Ludzie nowej organizacji. Wzory kultury organizacyjnej wysokiej tolerancji niepewności*, p. 23 (1998).
3. PN-ISO 31000:2012, *Zarządzanie ryzykiem -- Zasady i wytyczne*, (2012).
4. M. Kiedrowicz, *Location with the use of the RFID and GPS technologies - opportunities and threats*, GIS ODYSSEY 2016, pp. 122-128, (2016).
5. 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).
6. 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).
7. 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**, DOI: 10.1051/matecconf/20167604010 (2016).
8. J. Stanik, J. Napiórkowski, R. Hoffmann, *Zarządzanie ryzykiem w systemie zarządzania bezpieczeństwem organizacji*, Zeszyty Naukowe Uniwersytetu Szczecińskiego – Ekonomiczne Problemy Usług, (2016).
9. J. Gołębiewski, *Zarządzanie kryzysowe w świetle wymogów bezpieczeństwa*, pp. 120-121, (2011).
10. D. Wróblewski (ed.), *Przegląd wybranych dokumentów normatywnych z zakresu zarządzania kryzysowego i zarządzania ryzykiem wraz z leksykonem*, p. 161, (2014).
11. 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,

[20] ISO 31000:2009 does not recommend any model or sample documentation forms concerning risk management, but provides only general recommendations on risk identification. Given the importance of this issue, it was outlined in more detail in the article.

[21] Example of risk registers can be found in *Risk Management Guidelines Companion to AS/NZS 4360:2004*, replaced by current ISO 31000 [3].

(eds) B.F. Kubiak and J. Maślankowski, pp. 231-249, (2015).

12. J. Hash, *Risk Management Guidance For Information Technology Systems*, ITL Bulletin, (2002).
13. T. Trajdos, *Matemetyka*, (1993).
14. S. Nowosielski, *Modelowanie procesów gospodarczych w literaturze i praktyce*, (in:) Podejście procesowe w organizacjach, (ed.) S. Nowosielski, (2009).
15. J. Stanik, T. Protasowicki, KKIO - Od procesów do oprogramowania: badania i praktyka, *Metodyka kształtowania ryzyka w cyklu rozwojowym systemu informatycznego*, (2015).
16. 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).
17. J. Zawiła-Nadźwiecki, *Metoda TISM-BCP – Total Security Management. Business Continuity Planning*, (2003).
18. B. Bruegge, A. Dutoit, *Inżynieria oprogramowania w ujęciu obiektowym. UML, wzorce projektowe i Java*, (2011).
19. M. Piotrowski, *Notacja modelowania procesów biznesowych*, (2007).
20. 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).
21. M. Kiedrowicz, T. Protasowicki, J. Stanik, *Wybrane aspekty standaryzacji w ochronie publicznych zasobów informacyjnych i świadczonych usług w kontekście społeczeństwa informacyjnego*, Zeszyty Naukowe Uniwersytet Szczeciński.. – Ekonomiczne Problemy Usług, vol. **113**, pp. 113-130, (2014).
22. 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).
23. M. Kiedrowicz, *Uogólniony model danych w rozproszonych rejestrach ewidencyjnych*, Roczniki Kolegium Analiz Ekonomicznych, vol. **33**, pp. 209-234, (2014).
24. 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).
25. 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).
26. R. Kasprzyk, A. Stachurski, *A concept of standard-based vulnerability management automation for IT systems*, Computer Science and Mathematical Modelling, pp. 33-38, vol. **3**, (2016).
27. R. Kasprzyk, M. Maj, Z. Tarapata, *Przestępstwa w cyberprzestrzeni. Aspekty techniczne i prawne*. (in:) Przestępczość w XXI wieku. Problemy technologiczno-informatyczne., pp. 527-539, Warszawa, (2015).
28. M. Kiedrowicz, *Objects identification in the information models used by information systems*, GIS ODYSSEY 2016, pp. 129-136, (2016).
29. Z. Tarapata, *Models and algorithms for knowledge-based decision support and simulation in defence and transport applications*, Wojskowa Akademia Techniczna, Warszawa, (2011)
30. 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)
31. Z. Tarapata, R. Kasprzyk, Graph-based optimization method for information diffusion and attack durability in networks, *RSCTC 2010*, Lecture Notes in Artificial Intelligence, vol. **6086**, pp. 698-709 (2010)
32. M. Kiedrowicz, T. Nowicki, R. Waszkowski, Z. Wesolowski, and K. Worwa, *Method for assessing software reliability of the document management system using the RFID technology*, 20th International Conference on Circuits, Systems, Communications and Computers, MATEC Web of Conferences, vol. **76**, DOI: 10.1051/matecconf/20167604009 (2016).
33. M. Kiedrowicz, T. Nowicki, R. Waszkowski, Z. Wesolowski, and K. Worwa, *Business processes in the RFID-equipped restricted access administrative office*, 20th International Conference on Circuits, Systems, Communications and Computers, MATEC Web of Conferences, vol. **76**, DOI: 10.1051/matecconf/20167604003, (2016).
34. M. Kiedrowicz, T. Nowicki, R. Waszkowski, Z. Wesolowski, and K. Worwa, *Software simulator for property investigation of document management system with RFID tags*, 20th International Conference on Circuits, Systems, Communications and Computers, MATEC Web of Conferences, vol. **76**, DOI: 10.1051/matecconf/20167604012 (2016).
35. R. Hoffmann, M. Kiedrowicz, J. Stanik, *Evaluation of information safety as an element of improving the organization's safety management*, 20th International Conference on Circuits, Systems, Communications and Computers, MATEC Web of Conferences, vol. **76**, DOI: 10.1051/matecconf/20167604011, (2016).
36. M. Kiedrowicz, *Rejestry i zasoby informacyjne wykorzystywane przez organy odpowiedzialne za wykrywanie i przeciwdziałanie przestępczości*, (in:) Jawność i jej ograniczenia, (ed.) G.Szpor, Monografie Prawnicze, (vol. IX), pp. 170-264, (2015).
37. M. Kiedrowicz, *Dostęp do publicznych zasobów danych - Big data czy Big brother*, (in:) INTERNET. Publiczne bazy danych i Big data, (ed.) G. Szpor, pp. 15-39, (2015).
38. M. Kiedrowicz, *The importance of an integration platform within the organisation*, Zeszyty Naukowe, vol. **46**, pp.83-94, (2014).
39. M. Kiedrowicz, T. Nowicki, R. Waszkowski, *Business process data flow between automated and human tasks*, 3rd International Conference on Social Science (ICSS 2016) December 9–11 2016, pp. 471-477, (2016).