Models and method for the risk assessment of an intellectual resource

MACIEJ KIEDROWICZ, JERZY STANIK
The Faculty of Cybernetics
Military University of Technology
00-908 Warsaw, Kaliskiego Str. 2
POLAND
maciej.kiedrowicz@wat.edu.pl, jerzy.stanik@wat.edu.pl

Abstract: - The objective of the article is to show the impact of various categories of risk factors related to intellectual resources, i.e. the components of intellectual capital, on their safety and going concern. Following an analysis of the literature on this subject and the authors' own observations, an attempt was made to define three types of risk models related to intellectual assets. A substantial part of the study was devoted to the methodology of risk assessment of the intellectual resource. The presented approach considers various categories of risk factors, resulting from both the architecture of the intellectual resource as well as other elements used in the processes and areas of intellectual capital management. The models outlined in this article could be the starting point for developing the methodology of risk assessment of the intellectual assets and appropriate policies of an organization, e.g. its information security, risks or quality, which may in turn constitute input values for developing the risk management system related to the intellectual capital of such organization.

Key-Words: - Risk, Intellectual Resources, Intellectual Assets, Information Security,

1 Introduction

It is currently an indisputable and common belief that the proper use of ***intellectual assets*** of a company as well as creativity and innovativeness of its staff may lead to stable and competitive activities of such company and contribute to economic success. The condition, which is not always fully appreciated, but which determines the whole process of creating and protecting innovative activities of people, is to establish an appropriate strategy for the intellectual property management and risk management system related to the company's intellectual resources. In the absence of efficient framework for the protection of intellectual property rights, both innovativeness and creativity are hampered and the number of investments drops.

This phenomenon has contributed to the writing of this article, which includes elements of the risk management process in terms of quality and security of intellectual assets in the company. Experience shows that the costs resulting from not being familiar with the topic (or even being an ignoramus) may be substantial. On the other hand, the benefits of applying the methodology for the risk management of intellectual assets and intellectual property increase, since intangible assets - considered the profit generating factors - grow in significance. Therefore, the companies are forced to look for new paradigms of risk management [1], which shall concentrate more on intangible assets.

1.1 The concept of an intellectual resource of the organization

The concept of the intellectual resource is closely related to the idea of intellectual capital. Review of the body of literature allows to state that the intellectual capital is the property emerging on the basis of knowledge. It constitutes the sum of many intangible assets, which shape the market value of a company and which are often referred to as the knowledge capital or intellectual matter. Particular elements that create the intellectual capital are shown in table 1.

Table 1. Elements of intellectual capital

Human capital	Client capital (relationship)
– know-how – skills – education – professional qualifications – experience – professional predispositions – resourcefulness, enthusiasm – innovativeness – capability, motivation	– trademark – clients – customer loyalty – business name – distribution channels – collaboration with other companies – concession contracts – beneficial contracts – franchising contracts
Organizational (structural) capital	
Intellectual property: – patents and copyrights	Infrastructural assets: – philosophy of

– rights to designs – trade secret – brand name – distinctive services	management – organizational culture – management processes – information system – financial relations

Source: own elaboration.

Human capital and organizational capital operate together to create the client's capital (Table1). At the heart of all these intellectual capital elements, which overlap, there are intellectual resources [3] that create the goodwill (Fig.1).

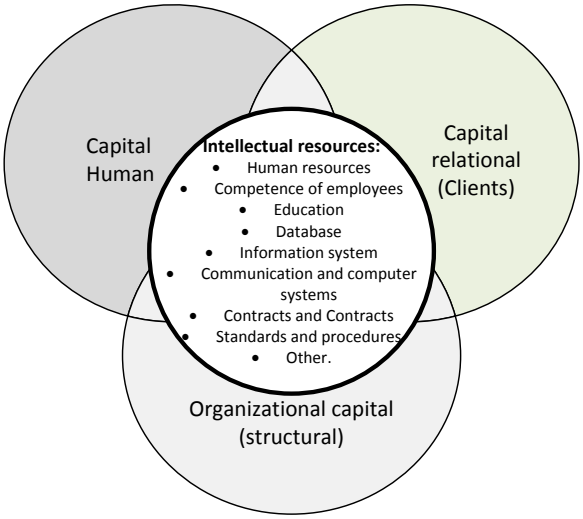

Fig.1. Intellectual resources in comparison with the components of intellectual capital.

Intellectual assets/resources are often referred to as the wealth or treasure of an organization and seen as items of individual components of intellectual capital.

The majority of authors agree that the *intellectual resources* play a key role among the components of intellectual capital. They constitute intellectual assets, which are the sum of knowledge of employees or separate groups (structures) of employees [4, 8, 9] and which the organization uses in its business activities by applying the currently available technologies (Fig. 2).

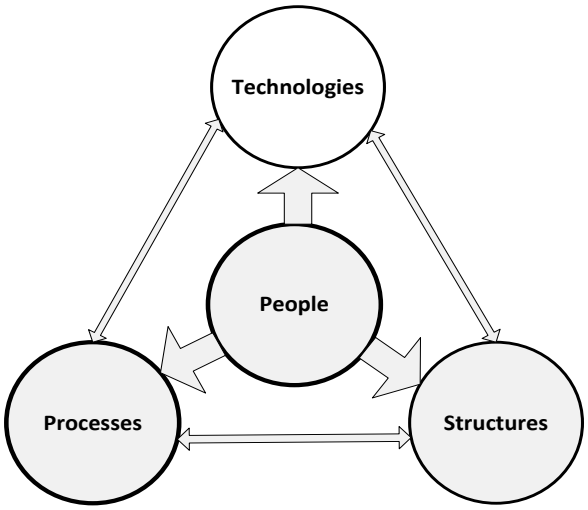

Fig.2. Basic elements of the organization and correlations between them.

For the purposes hereof, the following definition of the intellectual resource was adopted:

Intellectual resources of the organization are its *intellectual assets*, such as d ata, information or knowledge (Fig.3);

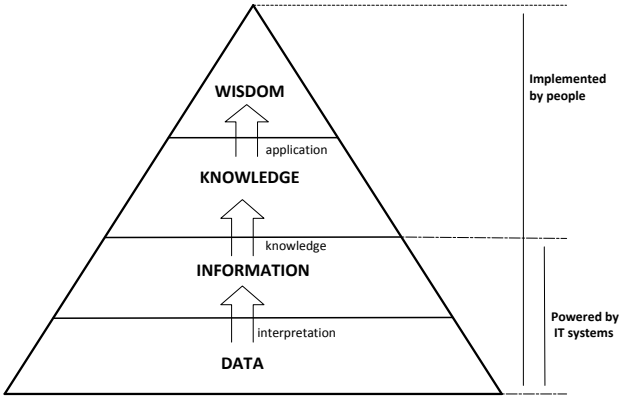

Fig.3. Basic types of intellectual resources and correlations between them. Source: own elaboration.

Whereas [7, 10, 12]:

- The data constitute raw facts, numbers and events, not subject to any analysis, on the basis of which the information may be developed. Clean unprocessed data have little practical meaning. The development of IT technologies significantly accelerates the data management process.
- The information is an abstract value, which may be:
  - stored in certain objects,
  - transferred between certain objects,
  - processed in certain objects and used to control certain objects, where the objects shall be deemed to mean living organisms, processes, devices and systems of such objects.

- The knowledge is created after drawing conclusions from available data and information. Extensive knowledge of a given matter leads to wisdom.
- Wisdom means practical use of knowledge.

A person, paper or electronics are carriers of every intellectual resource [13, 14].

2. Review of models for the risk assessment related of the intellectual resource

Specialist literature [11, 15, 16, 18, 21] contains description of a number of the model for risk assessment, which are based on norms, experiences and expert knowledge. A number of components included in the risk assessment process constitutes basis for such models. The first and basic component is a broad list of risks and register of risks, which may affect the predefined modeling goals - regardless of whether their sources are controlled by the organization or not [22]. Another element are specified criteria for risk assessment, which shall be applied at the stage of analysis, estimation and finally evaluation of such risk. Such criteria usually include the following:

- definitions of consequences (nature, type and manner of measurement),
- definitions of probabilities (type and manner of measurement),
- categories of risk level (manner of determination),
- categories of evaluation (determination of acceptable or tolerable risk level).

Another element are domain-specific models, e.g. information security, ICT security or ongoing concern. These models constitute a "good" starting point for building multi-component[1] models for risk assessment.

2.1. Two-dimensional model for risk assessment

The model for risk assessment shall be the following [15]:

RISK = PROBABILITY x VALUE OF LOSS

$$\mathcal{R} = P(z) \cdot S(z) \qquad (1)$$

where:

$P(z)$ – probability of risk occurrence,

$S(z)$ – value of losses (impact) caused by the actual risk,

$\mathcal{R}$ – risk assessment.

In light of the above definition, the risk assessment process means an analysis allowing to define whether the level of a given risk (understood as the sum of risks) is acceptable or not. The risk analysis comes down to the use of the so-called Risk Matrices as the risk evaluation tools. They are composed of the two combined (usually five-step) scales: probability and effects, allowing to determine the level of acceptable risk (Fig. 4). The risk matrix provides appropriate grounds for planning and implementing risk mitigation measures.

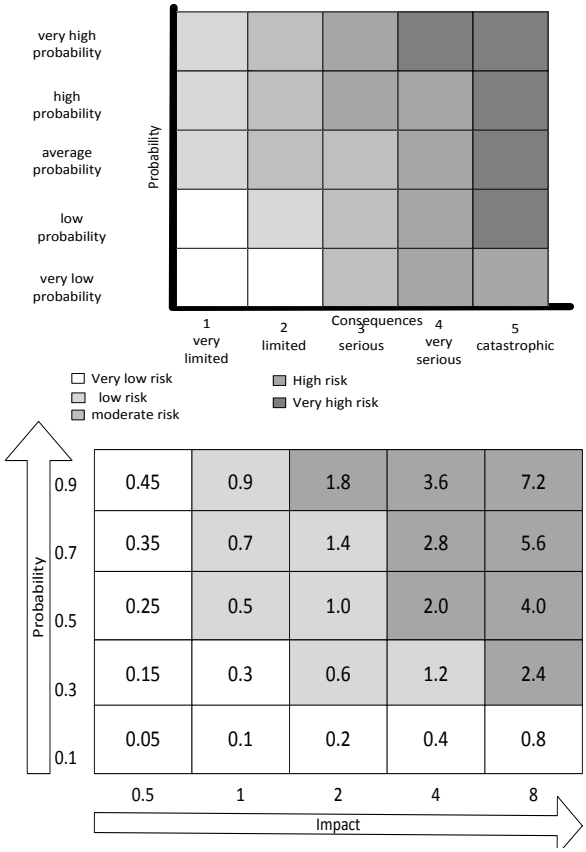

Fig.4. Model risk matrices.

Figure 5 shows the model risk profile for the selected risk factors modified as a result of undertaking appropriate management actions.

[1] The name is derived from decision-making variables, which are taken into consideration in the risk assessment process.

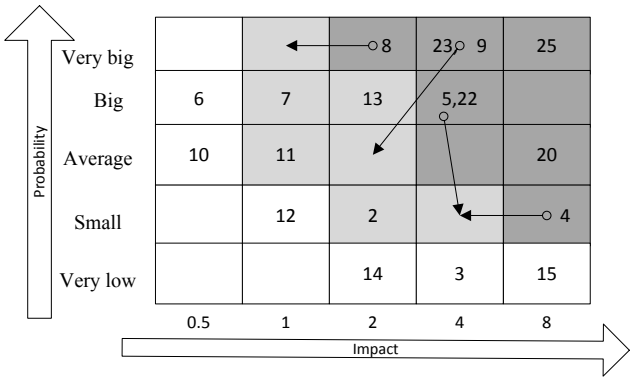

Fig.5. Model risk profile.

The risk model (profile) provides appropriate grounds for planning and implementing risk mitigation measures. The risk assessment process includes an analysis of advantages and disadvantages of the proposed solutions and may be followed by the necessary conclusions: should a given solution be applied or not, to what extent the risk will decrease and what will be the costs related thereto.

2.2. Three-dimensional model for risk assessment

Apart from any attempts to define the concept of risk, it simply means:

- prospective consequences of wrong decisions,
- poor quality of human capital in the organization,
- inadequacy of information, based on which the decisions are to be made, no vertical and horizontal communication within the organizational structure, loss of information, infringement of information confidentiality,
- inadequate organizational structure, lack of predefined scope of duties of the managerial staff and employees, imprecisely defined scope of duties, lack of formal duties, inefficient system for information flow,
- ***the risk*** that technologies, e.g. information or IT, used in a given organization (regardless of its type and scale of activity):
  - do not satisfy business criteria,
  - were not properly implemented and do not operate in compliance with the assumptions,
  - do not provide appropriate integrity, security and access to intellectual resources,
  - do not meet the requirements included in various policies related to security, quality, ongoing concern, etc.,

and, additionally, the model may be used to measure the risk of:

- events that occurred,
- potential occurrence of situations,
- maintenance of assigned features or properties.

Well-targeted and consistent prevention measures are the best way to avoid the effects of potential risks and increase chances for improving efficiency or implementing objectives of the organization in a smooth manner. To come up with the right definition of the risk of intellectual resources and risk model shall be the starting point for indicating all methods of risk assessment and risk level management.

The fundamental elements of the three-component model for risk assessment are the following:

- Register of intellectual resources subject to protection,
- Security model for intellectual resources,
- Register of security mechanisms to be implemented - technical and organizational security measures.

The starting point for building the model for risk assessment, ensuring completeness of the presented approach, shall be the security model for intellectual resources shown in figure 6.

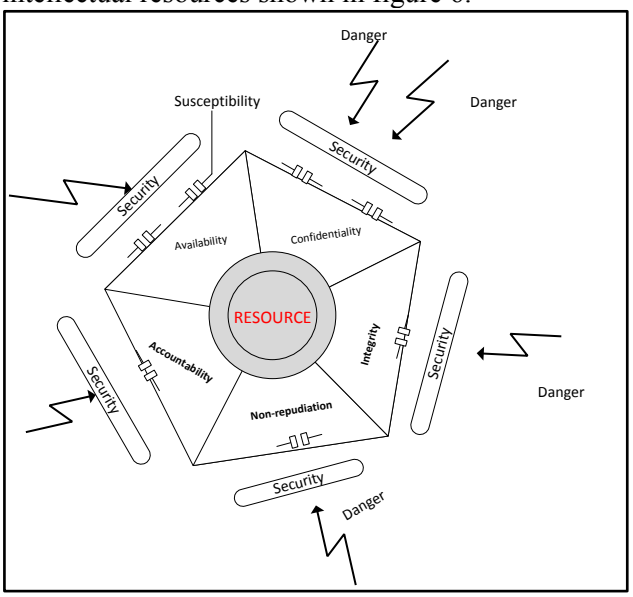

Fig.6. Security model for intellectual resources.

The security model for intellectual resources shown in figure 6 is based on the following components:

- Intellectual resources subject to protection, including the assigned security attributes,
- Valuation of the resource (WS) in the context of potential losses in case of the loss of the assigned security attributes,

- Set of typical risks (Z) related to the resource (it is recommended to pay special attention to the sources of personal risks),
- Susceptibility (P) of the resource within different areas of security,
- The set of security mechanisms/measures currently assigned to the resource (MZ).

On the basis of the above-mentioned data, it is possible to determine the status (situation) of the intellectual resource in terms of a possibility of losing the security attributes assigned thereto, which may be illustrated with the Cartesian product$\langle WS, \mathbb{P}, \mathbb{Z} \rangle$.

The following formula is used to reflect the risk model [15]:

$$\mathcal{R} : \langle WS, \mathbb{P}, \mathbb{Z} \rangle \rightarrow \mathcal{N} \quad (2)$$

where: N is a set of permitted values in the risk assessment process related to the information resource.

The manner of risk assessment is shown in figure 7, which comprises four tables.

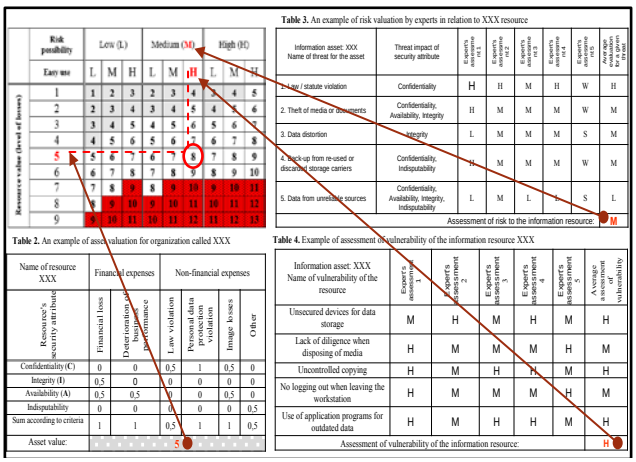

Fig.7. Diagram showing risk values for the intellectual resource.

In practice, it is believed that the information resource is safe if the following security attributes are satisfied [16]:

- Confidentiality (ISO 27001) - the information shall not be made available or disclosed to any unauthorized persons, entities or processes; only authorized persons may have access thereto;
- Integrity (ISO 27001) - accuracy and completeness of assets (resources); accuracy and completeness of information in line with its business impact, adopted assumptions and methods for processing;
- Availability (ISO 27001) - availability and usefulness of the resources upon r equest of an authorized entity; guarantee that only authorized persons have access to the information and assets related thereto, as the case may be;
- Authenticity - both the origin and content of data describing the object are as declared;
- Accountability - ability of the system to assign specific actions in the system to a natural person or process and place them in time;
- Non-repudiation - inability to negate the participation in data exchange, in whole or in part, by one of the entities involved in such exchange;
- Reliability (ISO 27001) - consistent, deliberate behavior and effects.

The main method for controlling such security attributes are the following types of audit: recurring, objective, based on clear metrics. To state whether the security attribute assigned to the intellectual resource is satisfied, two values shall be needed: residual risk[2] and acceptable risk[3]. If the value of residual risk is lower than the value of acceptable risk, it is considered that the security attribute was satisfied.

3 Multi-dimensional model for risk assessment

The following vector, described herein, shall be used as the model for risk assessment of the information resource $\overrightarrow{R_{Z_i}}$:

$$\overrightarrow{R_{Z_i}} = \langle \overrightarrow{R^1_{Z_i}}, \overrightarrow{R^2_{Z_i}}, \ldots \overrightarrow{R^J_{Z_i}} \rangle \in M_{m\times n} \times M_{m\times n}, \ldots \times M_{m\times n} \quad (3)$$

where:

- $\overrightarrow{R^1_{Z_i}}, \overrightarrow{R^2_{Z_i}}, \ldots \overrightarrow{R^J_{Z_i}}$ - vector coordinates $\overrightarrow{R_{Z_i}}$ describing particular areas of activities, where the intellectual resources are exposed to various types of risks, whichcreate a combination of linear risk elements of an intellectual system Z_i in the base of linear space$(M_{2\times 2}, \boldsymbol{R}, +, \cdot$. (e.g.: legal aspects, market, security, ongoing concern, IT, quality of the provided services, etc. - figure 8);
- $M_{m\times n}$ - matrix size m x n;
- $(M_{m\times n}, R, +, \cdot)$ - the vector space defined as the set of matrices M^{mxn} with an operator for adding matrices + and external operator · is the vector space over the body of real numbers R .

[2] Residual risk – the risk that remains after undertaking a certain action specified in the risk management procedure. Source: ISO Guide 73:2009 Risk Management – Vocabulary, definition 3.8.1.6.

[3]Acceptable risk – the level of risk which the organization may accept without any additional remedial actions or changes in its operations.

On the basis of the linear combination of the above formulas, it is evident that the impact of all dimensions of the analysis of risk of the intellectual resource divided into particular coordinates of the $\overrightarrow{R_{Z_i}^1}$, $\overrightarrow{R_{Z_i}^2}$, ... $\overrightarrow{R_{Z_i}^J}$ risk vector $\overrightarrow{R_{Z_i}}$ is the same. To specify the assessed level of the risk of the intellectual resource, it may be necessary to assign the weight of impact of particular vector coordinates on the final level of the risk of the intellectual resource and modify vector coordinates of such risk $\overrightarrow{R_{Z_i}}$ by applying the aforesaid weights of impact. The aforesaid issue was not discussed in the article. Due to the fact that the concept of the risk vector related to the intellectual resource and vector coordinates are already defined in algebra, $(M_{\mathrm{m\times n}}, \boldsymbol{R}, +, , \otimes)$ to determine total risks of the intellectual resource, it is essential to first set the values of $\overrightarrow{R_{Z_i}^1}$, $\overrightarrow{R_{Z_i}^2}$, ... $\overrightarrow{R_{Z_i}^J}$ and then - R_{z_i}.

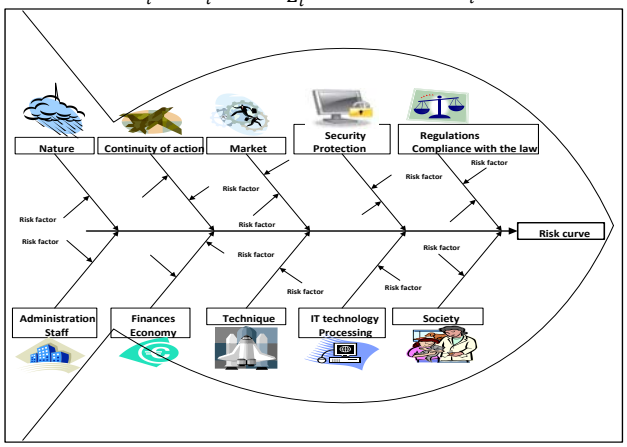

Fig.8. All areas of activity where the organization is exposed to risk.

In algebra, the risk of the $\overrightarrow{R_{Z_i}^1}$, $\overrightarrow{R_{Z_i}^2}$, ... $\overrightarrow{R_{Z_i}^J}$ vector coordinate $\overrightarrow{R_{Z_i}}$ related to the intellectual resource Z_i is $(M_{\mathrm{m\times n}}, \boldsymbol{R}, +, , \otimes)$ the number - $R_{Z_i}^1$; $R_{Z_i}^2; \ldots, R_{Z_i}^J \in \mathcal{R}$ equal to the length of a vector, i.e.:

$$R_{Z_i}^1 = \left\|\overrightarrow{R_{Z_i}^1}\right\|; R_{Z_i}^2 = \left\|\overrightarrow{R_{Z_i}^2}\right\|; \ldots; \ R_{Z_i}^J = \left\|\overrightarrow{R_{Z_i}^J}\right\| \quad (4)$$

The presented values $\overrightarrow{R_{Z_i}^1}$, $\overrightarrow{R_{Z_i}^2}$, ... $\overrightarrow{R_{Z_i}^J} \in \mathcal{R}$ define, in a quantitative manner, the magnitudes of all components of the risk of the intellectual resource Z_i. The magnitude of the risk of the intellectual resource Z_i may be defined as the vector module $\left|\overrightarrow{R_{Z_i}}\right|$:

$$\overrightarrow{R_{Z_i}} = \left|\overrightarrow{R_{Z_i}}\right| = \sqrt[2]{R_{Z_i}^{1\ 2} + R_{Z_i}^{2\ 2} + \cdots + R_{Z_i}^{J\ 2}} \quad (5).$$

4 Methodology of risk assessment of the intellectual resource

Assessment of the risk level concerning all intellectual resources of the organization is performed in the following steps:

1. Identification of risk factors - process of searching, identifying and describing risk areas and factors.
2. Determination of the level of factors having impact on the risk. The method considers such variants of factors, which - in the opinion of the authors - allow to assess the level of risk of the intellectual resources in a relatively objective and accurate manner. T herefore, the AHP[4] method is recommended.
3. Normalization of factors having impact on the risk.
4. Definition of the risk vector based on t he normalized risk components.
5. Determination of the weights of impact of particular factors on the total risk level for a given intellectual resource. The weights of impact are defined depending on the type of the intellectual resource processed by a given organization.
6. Determination of the weighted risk vector. The vector considers the impact of the resource on the risk of a given information/IT system.
7. Determination of the final risk level for a given information resource.

The following subchapters include the description of[5] points from 1-4 only. A general review of the risk assessment process related to the intellectual resource is shown in figure 9.

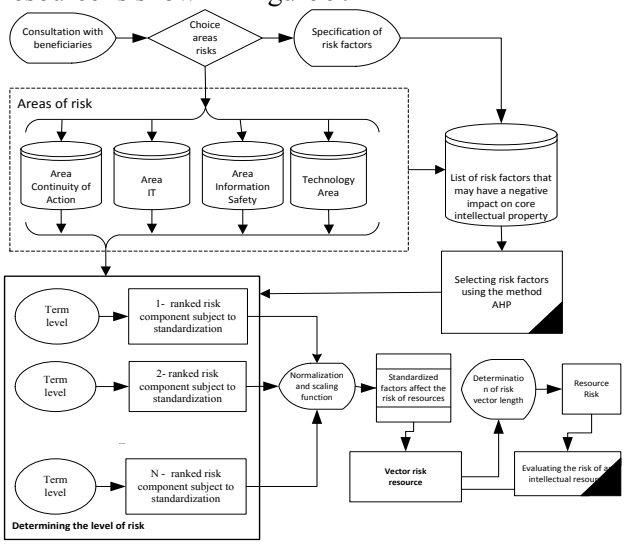

Fig.9. Risk assessment of the intellectual resource.

[4] Analytic Hierarchy Process (AHP).
[5] Issues 5-7 were omitted due to editorial requirements.

4.1. Identification stage

The point of risk identification is to make a complete list of risks resulting from possible events, which - depending on the circumstances - may create, prevent, limit, accelerate, delay or make it impossible to appropriately process the intellectual resource.

The risk identification process is a continuous action, since the risk or risk factors undetected on time may not only make it impossible to reach the goal, but also pose threat to the entire organization. Possible identification methods: measurements, discussions, simulations, experiences, expertise, laboratory research, detection systems, modeling, scenarios, questionnaires, forecasts, risks analyses, structures, solutions (weak and strong points, possibilities and needs). Possible risk sources: natural and technical threats, law defects (absence of appropriate regulations), bad habits, mentality of people, weakness of the organization, lack of training, low awareness of risks, lack of readiness, unprepared personnel, lack of system, unreal security standards, technical and technological gaps, in compliance with technological standards, operation errors, omission and neglection, indifference, incompetency, (system) corruption. The identification stage ends with an application of the AHP method. The result of the AHP method is the vector that orders the groups of risk factors related to the intellectual resource.

4.2. Stage of determination of factors having impact on the risk

During the risk assessment process, members of the risk analysis team examine such groups of factors and their attributes, which they believe allow to perform a relatively objective and accurate assessment of the risk level related to the intellectual resources [2]. Examples of methods for determining factors having impact on the risk are in table 2.

Table 2. Examples of methods for determining the level of factors in the "information security" area

Risk factor	Method for determining the level
Availability of intellectual resources λ_{Z_i}	The availability of the intellectual resource Z_i refers to the availability of certain actions that may be undertaken within the stipulated period of time and upon request of an authorized entity in a given company. The availability of data in an IT system Z_i is expressed through the availability classification $\lambda \in \Lambda$ of the intellectual resources Z_i and marked accordingly λ_{Z_i}. The set of classes of the intellectual resource Z_i is called L = {I, II, III, IV, V}. I – an intellectual resource Z_i, in case of which the expected availability is 99.99% per year, whereas the maximum one-time system unavailability is not longer than 30 minutes, V – an intellectual resource Z_i, in case of which the expected availability is below 70% per year, whereas the maximum one-time system unavailabilityis longer than 3 weeks.
Confidentiality of the intellectual resource $-\alpha_{Z_i}$	The confidentiality of the intellectual resource Z_i refers to its non-disclosure to any parties unauthorized to obtain such information. The confidentiality of the intellectual resource Z_i is expressed in the availability classification $\alpha \epsilon$A and marked accordingly as α_{Z_i}. The set of confidentiality classes of the intellectual resource is called A = {A, B, C, D, E} A – defines the IT system & processes confidential data, whose disclosure may pose risk to human health or life, E – defines the IT system processing publicly available data.
Efficiency of the information security system $-\beta^{B}_{Z_i}$,	Efficiency of the intellectual resource Z_i called a product $\beta^{B}_{S_i} = d^{B}_{SM}(S_i) * \sum_j \left(\delta^{m}_{S_i} * \upsilon^{k^j}_{S_i}\right)$; where: j – number of the next criterion for assessment of efficiency of the security monitoring system, $\delta^{m}_{S_i}$ – priority *j–th*criterion for assessment of efficiency of the security monitoring system with respect to the system S_i, $\upsilon^{k^j}_{S_i}$ – value *j–th* criterion for assessment of efficiency of the security monitoring system with respect to the system S_i,
Fulfillment of requirements defined in the information security policy - $\eta^{B}_{Z_i}$	The set of requirements of the O Organization policy is a finite set, $W^{B}_{P(O)} = \{w_1, w_2, \ldots w_{M^B}\}$, where: M^B is the number of requirements in the security policy related to the intellectual resource. For each requirement of $w_m \epsilon W^{B}_{Z(i)}$ the value of the requirement priority related to the intellectual resource is defined Z_i.. The requirement priority $w_m \epsilon W^{B}_{Z(i)}$ is the number $p^{m}_{Z_i} \in \{0,1, \ldots 5\}$ The following percentage value Z_i constitutes the fulfillment of the intellectual resource policy: $$\eta^{B}_{S_i} = \frac{\sum_{m=1}^{\overline{W^{B}_{P(O)}}} \left(p^{m}_{S_i} * s^{m}_{S_i}\right)}{\sum_{m=1}^{\overline{W^{B}_{P(O)}}} p^{m}_{S_i}}$$ where: $W^{B}_{S_i}$ – set of security requirements for the intellectual resource Z_i , $p^{m}_{S_i}$– requirement priority *m* related to the system S_i, $s^{m}_{S_i}$ – requirement fulfillment *m* with respect to the system S_i.

Source: own elaboration.

4.3. Normalization of factors having impact on the risk

Due to the fact that particular risk factors within the distinguished areas belong to different sets of values, it is necessary to introduce the following function: ξ or a set of functions: $\xi\epsilon\Xi$, which clearly transpose such components into a uniform range of values. The normalization function is called the family of functions: $\xi\epsilon\Xi$

$$\xi{:}X\longrightarrow[1,\,2,\,\ldots,\,N] \tag{6}$$

Forms of the normalization functions from the family of the following functions: Ξ should be defined in such a manner so as to: reflect their values in the range: [1,..., N] and maintain appropriate proportions of their impact on the total risk of the resource, while considering the set X of all specified risk factors. The set$X$ should be divided into subsets representing the distinguished areas/aspects.

The proposed ranges are not obligatory; they may be customized. Model forms of the normalization functions are in table 3.

Table 3. Model forms of the normalization functions in the information security area.

A. For function $\xi\epsilon\Xi^{B}$	accessibility$\xi_{a}(\lambda_{Z_i})=$	data confidentiality $\xi_{a}(\alpha_{Z_i})=$	compliance with PB requirements $\xi_{\eta}^{B}(\eta_{Z_i}^{B})=$	security monitoring $\xi_{\eta}^{B}(\beta_{Z_i}^{B})=$
normalization function	$\begin{cases}1, \text{when } \lambda_{Z_i}=\text{V}\\ 7, \text{when } \lambda_{Z_i}=\text{IV}\\ 13, \text{when} \lambda_{Z_i}=\text{III}\\ 19, \text{when } \lambda_{Z_i}=\text{II}\\ 24, \text{when } \lambda_{Z_i}=\text{I}\end{cases}$	$\begin{cases}1, \text{when } \alpha_{Z_i}=\text{E}\\ 7, \text{when } \alpha_{Z_i}=\text{D}\\ 13, \text{when } \alpha_{Z_i}=\text{C}\\ 19, \text{when } \alpha_{Z_i}=\text{B}\\ 24, \text{when } \alpha_{Z_i}=\text{A}\end{cases}$	$1+9\left(1-\frac{\eta_{Z_i}^{B}}{100\%}\right)$	$10-\sqrt[2]{\frac{\beta_{Z_i}^{C}}{2}}$

Source: own elaboration.

4.4. Risk vector of the information resource and its magnitude

Since the grounds for the vector space are defined $(M_{\mathrm{m}\times\mathrm{n}},\boldsymbol{R},+,\cdot)$ in algebra $(M_{\mathrm{m}\times\mathrm{n}},\boldsymbol{R},+,,\otimes)$, it is possible to introduce the concept of the risk vector of the intellectual resource Z_i. The risk vector of the intellectual resource Z_i in algebra $(M_{\mathrm{m}\times\mathrm{n}},\boldsymbol{R},+,,\otimes)$ is called the vector $\overrightarrow{R_{P_i}}\in M^{mxn}$, which is a linear combination of elements of the risk of the information resource Z_i in the linear space base $(M_{\mathrm{m}\times\mathrm{n}},\boldsymbol{R},+,\cdot)$:

$$\overrightarrow{R_{Z_i}}=\xi_{\alpha^1}\left(\alpha_{Z_i}^{1}\right)\cdot\overrightarrow{\alpha^1}+\xi_{\alpha^2}\left(\alpha_{Z_i}^{2}\right)\cdot\overrightarrow{\alpha^2}+\cdots+\xi_{\alpha^J}\left(\alpha_{Z_i}^{M}\right)\cdot\overrightarrow{\alpha^M} \tag{7}$$

The dimension of algebra $(M_{\mathrm{m}\times\mathrm{n}},\boldsymbol{R},+,,\otimes)$ is: $\dim(M_{\mathrm{m}\times\mathrm{n}},\boldsymbol{R},+,,\otimes)=M$.

Based on the fact that the dimension of algebra $(M_{\mathrm{m}\times\mathrm{n}},\boldsymbol{R},+,,\otimes)$ is M, it is evident that M of base vectors in the vector space does exist $(M_{\mathrm{m}\times\mathrm{n}},\boldsymbol{R},+,\cdot)$ in algebra $(M_{\mathrm{m}\times\mathrm{n}},\boldsymbol{R},+,,\otimes)$, defined in the following way:

$$\overrightarrow{\alpha^1}=\begin{pmatrix}1 & \cdots & 0^n\\ \vdots & \ddots & \vdots\\ 0^m & \cdots & 0^M\end{pmatrix};\ \ldots;\ \overrightarrow{\alpha^M}=\begin{pmatrix}0 & \cdots & 0^n\\ \vdots & \ddots & \vdots\\ 0^m & \cdots & 1\end{pmatrix} \tag{8}$$

On the basis of the linear combination of the above formula, it is evident that the impact of all M dimensions of the risk analysis of the intellectual resource Z_i, the obtained risk vector $\overrightarrow{R_{Z_i}}\in M^{mxn}$ is the same. Therefore, to specify the assessed risk level of the intellectual resource Z_i, it may be necessary to assign the weights of impact of particular risk components on the final level of the risk of the intellectual Z_i resource and modify risk vector coordinates $\overrightarrow{R_{Z_i}}\in M^{mxn}$ by applying the aforesaid weights of impact. The issue was not discussed in this article.

4.5. Determination of the final risk level for a given resource

Since the concept of the risk vector of the intellectual resource is defined Z_i i n algebra $(M_{\mathrm{m}\times\mathrm{n}},\boldsymbol{R},+,,\otimes)$ it is possible to finally introduce the definition of the total risk of the intellectual resource Z_i. The risk of the information resource Z_i in algebra $(M_{\mathrm{m}\times\mathrm{n}},\boldsymbol{R},+,,\otimes)$ is the number $R_{Z_i}\in\mathcal{R}$ equal to the length of the vector being the risk vector of the intellectual resource,Z_i i.e.:

$$R_{Z_i}=\left\|\overrightarrow{R_{Z_i}}\right\| \tag{9}$$

The presented value R_{Z_i} defines, in a quantitative manner, the value of the risk of the intellectual information Z_i, which constitutes the result value of the method for analyzing the risk of the intellectual resource described in this article Z_i. For the purpose of presenting the risk level, in a qualitative manner, determined by using the above semi-quantitative method, the following risk ranges may be adopted: $R_{Z_i}>70$ - catastrophe risk, $R_{Z_i}\in(60,\ldots,70]$ - very high risk, $R_{Z_i}\in(50,\ldots,60]$ - high risk, $R_{Z_i}\in(40,\ldots,50]$ - medium risk, $R_{Z_i}\in(30,\ldots,40]$ - low risk, $R_{Z_i}\in(20,\ldots,30]$ - very low risk, $R_{Z_i}<20$ – residual risk.

5 Evaluation of the risk of the intellectual resource

The action consists in a comparison of the results of the risk analysis, including the adopted criteria for appropriate classification of the risk (acceptable,

tolerable and non-tolerable risk level). Potential methods for visualizing the risk of the intellectual resource are shown in figure 10.

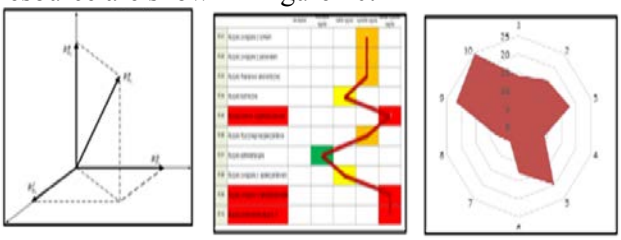

Fig.10. Methods for visualizing the risk of the intellectual resource

The primary objective is to provide data that constitute grounds for making a decision on further procedure with the risk (whether to abandon it or not, and if not, to what extent it should be processed). The risk evaluation process provides a summary of the current activities (risk identification) and an indication which risk or group of risks should be further processed and with respect to which it would be enough to apply present control measures.

The risk evaluation has significant impact on the decision-making process. The results of the risk analysis constitute grounds for making a decision on which risks and to what extent require the implementation of an appropriate algorithm for handling them and determining their priorities by a secretarial unit. Subsequently, the established levels of risk should be compared with their criteria, including the context determined at the beginning. In this case, the evaluation process allows to determine the method for handling a particular risk.

During the risk assessment process, each risk has to be classified and compared with its tolerable and acceptable value. However, it is also important to first adopt certain criteria that may help to clearly identify serious risk, which calls for strong reaction. It is a step towards identifying such serious risk. The risk records shall be established based on the risk evaluation process allowing to rationalize the risk management and hence emergency management.

Summary

The intellectual resources are in all areas of the intellectual capital of the company. They constitute hidden potential, which exists in modern organizations and helps to create best conditions for their development as well as in traditional organizations of different sizes. The extent to which the intellectual assets are considered significant is also determined by the subject of activities and segment in which a given company operates.

When assuming that the risk constitutes certain objective regularity characterizing the real world, in the age of rapid IT growth as well as more and more common application of IT systems for intellectual resource management, it becomes necessary to develop efficient models and methodologies for risk assessment of the intellectual resources, where the risk is considered a threat that the applied information technology may not function in line with our expectations. The knowledge of the risk level related to particular intellectual resources allows to efficiently manage such risk by using dedicated models and methods.

Nowadays, the intellectual capital management is considered a basic tool for future management and provides an opportunity for radical reorientation of the way of thinking and acting of every entity. On the other hand, the management of the intellectual resources may provide added value for the company, such as: increase of the intellectual capital, possibility of eliminating errors, increase of innovativeness, promotion of knowledge, management of knowledge, increase of creativity and competitiveness.

The issues related to the analysis, estimation and management of the intellectual resource risk still remain obscure in many companies. Nowadays, the companies need to face a lot of new challenges. The product whose characteristics may be easily copied does not play a significant role: the real competitive advantage is based on knowledge. Therefore, it is in the best interest of the company to introduce or improve the risk management system related to its intellectual capital.

The models and methodologies for the risk assessment of the intellectual resource described herein are characterized by relatively high complexity due to the necessity of applying mathematical apparatus. This is caused by a number of factors having impact on the risk level of the intellectual resource. It should be also stressed that the deliberations included herein are for informational purposes only, thus, a detailed and formal description of certain issues was omitted. The purpose was to outline the concept other than the traditional view of the matters related to quantification of threats and risk assessment.

References

[1] R. Hoffmann, M. Kiedrowicz, J. Stanik, Risk management system as the basic paradigm of the information security management system in an organization, *20th International Conference on Circuits, Systems, Communications and*

Computers, MATEC Web of Conferences, vol. 76, (2016).

[2] R. Hoffmann, M. Kiedrowicz, J. Stanik, Evaluation of information safety as an element of improving the organization's safety management, *20th International Conference on Circuits, Systems, Communications and Computers*, MATEC Web of Conferences, vol. 76, (2016).

[3] B. Kaczmarek, Kapitał intelektualny (wiedza) a kreowanie wizji przedsiębiorstwa, (in:) M.G. Woźniak (ed.), *Nierówności społeczne a wzrost gospodarczy. Kapitał ludzki i intelektualny*, part 2, Zeszyt nr 7, Uniwersytet Rzeszowski, Katedra Teorii Ekonomii, Rzeszów, (2005).

[4] 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).

[5] M. Kiedrowicz, Location with the use of the RFID and GPS technologies - opportunities and threats, *GIS ODYSSEY 2016*, pp. 122-128, (2016).

[6] M. Kiedrowicz, Objects identification in the information models used by information systems, *GIS ODYSSEY 2016*, pp. 129-136, (2016).

[7] M. Kiedrowicz (ed.). Zarządzanie informacjami wrażliwymi: Bezpieczeństwo dokumentów, wykorzystanie technologii RFID, Warszawa, (2016).

[8] 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).

[9] 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).

[10] M. Kiedrowicz (ed.). Zarządzanie informacjami wrażliwymi. Wybrane aspekty organizacyjne, prawne i techniczne ochrony informacji niejawnych, (2015).

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

[12] 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).

[13] M. Kiedrowicz, Uogólniony model danych w rozproszonych rejestrach ewidencyjnych, *Roczniki Kolegium Analiz Ekonomicznych*, vol. 33, pp. 209-234, (2014).

[14] 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).

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

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

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

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

[19] J. Stanik, J. Napiórkowski, R. Hoffmann, Zarządzanie ryzykiem w systemie zarządzania bezpieczeństwem organizacji. *Zeszyty Naukowe Uniwersytetu Szczecińskiego, Ekonomiczne Problemy Usług*, Szczecin, (2016).

[20] J. Stanik, T. Protasowicki, Metodyka kształtowania ryzyka w cyklu rozwojowym systemu informatycznego, *KKIO „Od procesów do oprogramowania: badania i praktyka"* (2015).

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

[22] D. Wróblewski, B. Połeć, Teoria i praktyka zarządzania ryzykiem – normy a regulacje w prawie miejscowym, (in:) D. Majchrzak (ed.), *Zarządzanie kryzysowe w wymiarze lokalnym. Organizacja, procedury, organy i instytucje*, AON, Warszawa, (2014), p. 206.