Evaluation of information safety as an element of improving the organization's safety management.

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

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

Abstract. The article discusses the problem of risk management in the context of safety of an organization's information assets. Assuming system of information risk management as a basic element of organization management in the aspect of information safety of modern organizations, this document focuses on methods and techniques of qualitative risk estimates. Basic standards and good practice from areas of risk management and ensuring information safety in the organization were recalled.

Introduction

Assuming that risk is an objective regularity that simple objects, processes and real world organizations are characterized by, in the age of rapid development of information technology and increasingly widespread use of IT systems, it becomes necessary to develop effective strategies, methods, evaluation systems or risk management related to operation of those facilities or systems, where the risk is defined as a threat, that the information technology used will not function the way it is expected to function.

Awareness of the risk level of organization's individual business processes or information systems within the organization allows for the effective management of such risk through the use of dedicated risk management systems for such purpose. In order to effectively manage security risk in the organization management it is necessary to determine, in a most objective manner, the level of such risk. Currently, there are many methods of the organization risk assessment, processes of information processing in the said organization or IT systems, but none of them, however, is a universal method, suitable for analysis of risks associated with an operation of both a small organization - a company, as well as complex organizations. In addition, none of the methods of analysis and risk assessment currently employed does not take into consideration, in a direct and comprehensive manner, factors such as quantitative, qualitative, economic or sociological - social factors, which on one hand is the strength of approaches currently employed through their focus on selected aspects of security, on the other hand, constitutes their weakness through far-reaching simplification of the adopted models or conditions for their development.

The proposed approach to risk assessment in security contained herein, also known as elements of "good practice" have been developed with the knowledge that along with the improvement in the system of risk management in information security and processes therein, they are subject to change.

This document defines the nature of risk, components of the system, model of risk management process, the role of risk analysis group and approaches to estimating safety of information.

1 The approach to risk assessment in information security

Risk assessment can be regarded as a process (see figure 1).

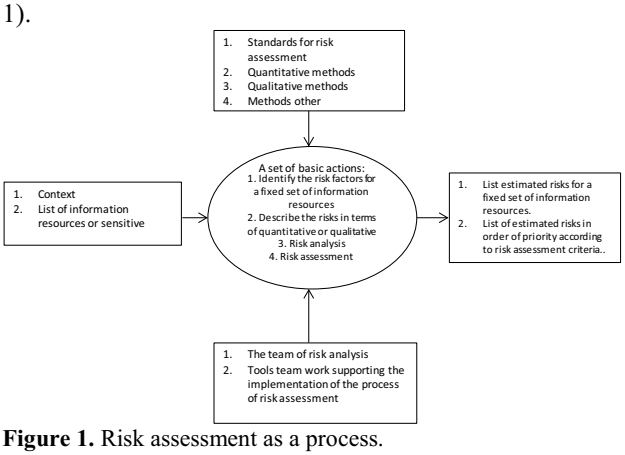

Figure 1. Risk assessment as a process.

Due to size limitations of this article only the basic elements of this process will be characterized in the remainder of this section, namely:

- Context,
- Identification of risk factors,
- Estimation of risk / Method of estimation.

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

2 Context

Establishing a context comes down to implementing the following tasks:

A. Determining the basic criteria needed for risk management in information security.
B. Defining the scope and limits of the risk management system.
C. Establish appropriate organizational structure dealing with risk management in information security.

As part of task A. (*Determination of basic criteria needed for risk management in information security*), the following operations need to be performed:

I. Choose or develop an appropriate approach to risk management, relating to the basic criteria, such as:
   1) criteria of risk management,
   2) results criteria,
   3) criteria of risk acceptance.

   While developing risk assessment criteria in information security in the organization, you should consider the following factors:
   1. The current map of business processes of the organization (figure 2.),
   2. Strategic business value of information processes,
   3. Importance of the information assets involved,
   4. Legal requirements resulting from the regulations and contractual obligations,
   5. A list of sensitive resources, as well as business and operational importance of their security attributes: availability, confidentiality, integrity, indisputability and accountability,
   6. Negative consequences for the image and reputation of the organization.

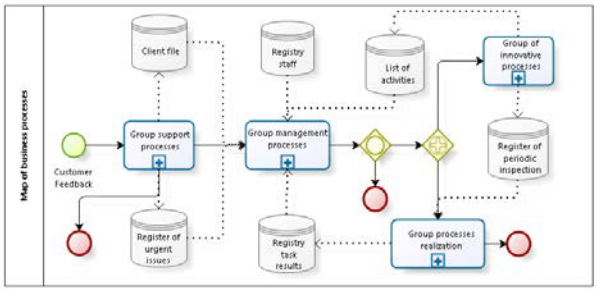

Figure 2. Sample map of business processes for a hypothetical organization.

II. Develop and determine the criteria for accepting risks taking into account the policies and objectives of the organization and the interest of the organization's employees.

III. Determine your own scale for levels of risk acceptance taking into account the following factors:
   – the criteria for accepting risks may include multiple threshold values having a desired target level of risk, but with the privilege of top company officers to accept risks exceeding the given level in certain circumstances,
   – criteria for accepting risk can be expressed as the ratio of estimated profit (or other business benefits) against the estimated risk;
   – different criteria for accepting risks may apply to different classes of risk, e.g. the risks which may result in non-compliance with regulations or provisions of law may not be accepted, whereas high risks may be accepted, if it is specified as a requirement under the contract;
   – criteria for accepting risks may include requirements relating to further additional proceedings, e.g. the risk may be accepted, if actions to reduce the risk to an acceptable level within a certain period of time are approved and carried out as an obligation.

IV. Determine a set of criteria for accepting risk, taking into account:
   – business criteria,
   – legal aspects and the resulting internal regulations,
   – usage,
   – technology,
   – finance,
   – social and human factors.

As part of task B. (*Defining a scope and limits of the risk management system)* the following steps need to be performed:

I. Determine the scope of the risk management process in information security, in order to ensure that the risk assessment takes into account all relevant assets.
   1. Basic assets:
      - Processes and business activities,
      - Information.
      - The supporting assets (which are based on the basic elements within the scope) of all kinds: Hardware, Software, Network, Personnel, Headquarter, and Organizational Structure.

II. In determining the scope and limits the organization should consider the following information:
   1. Strategic business objectives, strategies and policies,
   2. A list of key business processes,
   3. Information assets,
   4. Legal and contractual requirements resulting from the regulations and those applicable to the organization,
   5. The organization's information security policy,
   6. The organization's comprehensive approach to risk management,
   7. Locations of the organization and their geographical characteristics,
   8. Restrictions regarding the organization,
   9. Expectations of participants,
   10. Sociocultural environment,
   11. Interfaces (i.e. exchange of information with the environment).

As part of task C. (*Establishment of appropriate organizational structure dealing with risk management in information security*), it is necessary to perform the following:

I. The establishment and maintenance of the organization in addition to scope of responsibilities for the risk management process in information security. The main roles and responsibilities of such organizational structure are as follows:
   1. The development of the risk management process in the security information in a manner appropriate for the organization.
   2. Identification and analysis of the participants.
   3. Defining the roles and responsibilities of all parties, both internal and external in relation to the organization.
   4. Establishment of the required relationship between the organization and the participants, as well as interfaces to the highest management levels dealing with risk management (e.g. operational risk management) and interfaces to other relevant projects or activities.
   5. Defining decision escalation paths
   6. Defining accumulated records.

II. Establish / estimate whether the organization has the necessary Risk Analysis Team (RAT) - "*An agent of action*" - the necessary intellectual resources allowing for:
   1. Performing risk assessment and development of a strategy for dealing with risk.
   2. Define and implement policies and procedures, including the implementation of selected security.
   3. Monitoring of security measures.
   4. Monitoring the risk management process in information security.

3 Risk factors identification

The purpose of identifying risk factors is to determine what may happen causing potential loss, as well as gaining knowledge of how, where and why the loss might occur. The general scheme of the identification process is shown in Figure 3.

In order to carry out the identification of risk factors, it is recommended to conduct workshops often to discuss the list and definitions adopted for individual internal and external risks, to discuss the reasons for their occurrence and to determine the significance of individual risks for organizations and likelihood of their occurrence.

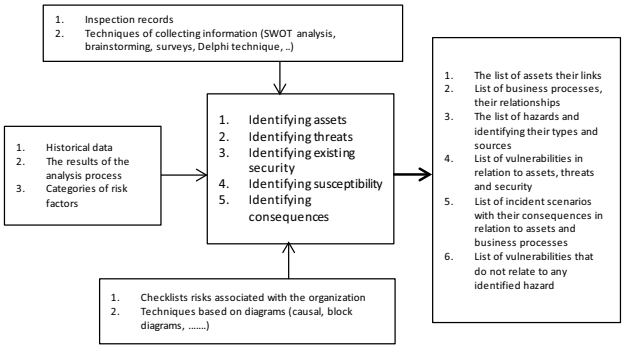

Figure 3. A general scheme of the risks identification process

These workshops allowed direct confrontation of opinions on internal and external risks inherent in the Organization formulated by the people having the most experience in working for the organization stemming from work in different areas of its operations. Collected results of the Workshops constitute a listing of risks associated with the activities of the Organization, according to importance of individual risks with detailed definitions assigned and causes for occurrence of particular risks. Manner of conducting individual risk identification is not a key element constituting its validity.

3.1 Identification of assets

Assets are anything of value to the organization and therefore require protection. When identifying assets it is recommended to take into account the fact that the information system also consists of elements other than hardware and software.

Identification of assets must be carrying out at the appropriate level of detail that will provide sufficient information for risk assessment. The level of detail used to identify the assets will have an impact on the total amount of information gathered during the risk assessment. This level of detail can be clarified in subsequent iterations of risk assessment. Each identified information resource should have its so-called "owner of the asset". The owner of the assets may not have the ownership of assets, however, (s)he is responsible for the development, maintenance and safety within the framework of assigned duties. The owner of assets is often the most appropriate person to assign a value to assets they have for the organization. After the identification of assets, the next step is a coordination of scale and criteria for the assignment of a specific point on the scale to all assets, based on the valuation of assets. Given the variety of assets operating in most organizations it is likely that part of the assets can be attributed to a specific value expressed in money, and for some you can only indicate a range of values, for example, from "very low" to "very high". The decision to use quantitative or qualitative scale depends on the preferences of the organization, but it is recommended to have a reference to the assets. Both types of assigning value can be used for the same assets. This work assumes, as the basis for valuation of assets, the costs incurred as a result of loss of confidentiality, integrity and

availability as consequences of an incident. It is also recommended to consider adequate repudiation, authenticity and reliability. Such an approach takes into account essential elements during valuation of assets, as a complement to a replacement cost, based on the estimation of negative business consequences that could result from incidents related to information security, assuming a particular set of circumstances. It is emphasized that this approach takes into account the consequences that are factors introduced into the risk assessment. After determining the criteria to be taken into account, you need to align the scale uniformly throughout the organization. The first step is a decision on the number of levels to be used in the scale. There are no rules regarding the selection of the most appropriate number of levels. More levels means greater detail, but sometimes too detailed diversity makes it difficult to obtain consistent estimates for the entire organization. Usually, any number between 3 (e.g. low, medium, high) and 5 can be used as long as it remains consistent with the organization's approach to the whole process of risk assessment. Each organization can define their own limits for asset values, such as "0-low", "0,5-average" or "1-high". It is recommended that these limits are estimated according to selected criteria limits (e.g. for a potential financial loss it is recommended that the limits are expressed in pecuniary values, but to consider such risks as the risk of personnel safety, a financial valuation may be complex and not always appropriate for each organization). Finally, only the organization can decide what is considered "low" or "high" consequence. A result, which can be disastrous for a small organization, may be small or even negligible for a very large organization. Cost values assigned to each security attributes are placed in the matrix in an orderly manner. An example is shown below. For more information on identifying and evaluation of assets in relation to information security can be found in Annex B of ISO 27005 standard: 2013.

Table 1. An example of asset valuation for organization called XXX

Name of resource XXX	Financial expenses		Non-financial expenses			
Resource's safety attribute	Financial loss	Deterioration of business performance	Law violation	Personal data protection violation	Image losses	Other
Confidentiality	0	0	0.5	1	0.5	0
Availability	1	0.5	0	0	0.5	0.5
Integrity	0.5	0.5	0	0	0	0
Indisputability	0	0	0	0	1	0.5
Sum according to criteria:	1.5	1	0.5	1	2	1
Asset value:	7					

3.2 Threat identification

The threat may be a potential cause of damage to assets such as information, processes and systems, and in consequence to the organization. Threat sources may be natural or human, accidental or deliberate. It is necessary to identify both accidental and deliberate threat sources. The threat may occur inside or outside the organization. It is recommended to identify risks of general nature and by type (e.g. unauthorized actions, physical damage, technical failures) and, where appropriate, to identify individual threats within the general category identified earlier. This approach means that it will not omit any threat, including the unexpected, whereas the workload will be limited. The following table shows examples of typical threats.

Table 2. Examples of typical threats

Type	Threat	Source
Violation of information security	Law / statute violation	Accidental threat, deliberate threat
	Media or documents theft	Deliberate threat
	Data distortion	Deliberate threat
	Back-up from re-used or discarded storage carriers	Deliberate threat
	Data from unreliable sources	Accidental threat, deliberate threat
	Software forgery	Accidental threat, deliberate threat

Some risks may relate to more than one type of assets. In such cases they may cause varying results depending on the assets to which they relate. Input data used to identify threats and to estimate the likelihood of occurrence can be obtained from the asset owners or users, employees of personnel departments, administrators of facilities and information security specialist, experts on physical security, as well as from other organizations, including legal institutions, meteorological services, insurance companies and government administration bodies. While describing threats it is proper to consider environmental and social aspects. It might be useful to take into account the listing of threats (specific for the organization of the industry) during completion of general threats, if these are applicable. Catalogs and statistics of threats can be shared by industry organizations, state governments, legal institutions, insurance companies, etc..

After conducting threat identification we need to align the scale and criteria for the assignment of a specific point on the scale to each threat, based on evaluation of threats. Given the variety of threat factors occurring in the organization it is likely that some part of risks can be assigned a specific value expressed in money, and for some you can only indicate a range of values, for example, from "very low" to "very high". Normally, any number between 3 (e.g. Low, medium, high) and 5 (e.g. very low, low, medium, high, very high) can be used as long as it remains consistent with the organization's approach to the entire process of risk assessment . Each organization can define their own limits for the risk values, such as "L - low," "M - medium" or "H - high." It

is recommended that these limits are estimated according to selected criteria limits (e.g. for a potential financial loss it is recommended that the limits are expressed in pecuniary values, but to consider such risks as the risk of personnel safety, a financial valuation may be complex and not always appropriate for each organization). Finally, only the organization can decide what is considered "low" or "high" consequence. A result, which can be disastrous for a small organization, may be small or even negligible for a very large organization. Threat values in the scope of individual security attributes assigned by experts are placed in the matrix in an orderly manner. An example is shown below. For more information about the types of threats and their evaluation can be found in Annex C of ISO 27005 standard: 2013.

Table 3. An example of risk valuation by experts in relation to XXX resource

Information asset: **XXX** Name of threat for the asset	Threat impact of security attribute	Expert's assessment 1	Expert's assessment 2	Expert's assessment 3	Expert's assessment 4	Expert's assessment 5	Average evaluation for a given threat
1. Law / statute violation	Confidentiality	H	H	M	H	H	H
2. Theft of media or documents	Confidentiality, Availability, Integrity	H	M	M	M	H	M
3. Data distortion	Integrity	L	M	M	M	M	M
4. Back-up from re-used or discarded storage carriers	Confidentiality, Indisputability	H	M	M	M	H	M
5. Data from unreliable sources	Confidentiality, Availability, Integrity, Indisputability	L	M	L	L	M	L
Assessment of risk to the information resource:							**M**

3.3 Identification of vulnerability

The very fact of existence of vulnerability does not cause any harm, as what is necessary is the risk using such vulnerability. The vulnerability, in case of which no relevant risk appears, may not require implementation of any security measures, yet, it is recommended to recognize it and monitor any changes with respect thereto. It is worth remembering that any security measure, which has been implemented incorrectly or functions incorrectly or is used incorrectly may cause vulnerability. The security measure may be efficient or inefficient depending on the environment, in which it operates. And vice verse, a threat without any matching vulnerability may not cause any risk. The vulnerability may be related to the properties of the assets, which may be used in an intentional manner or otherwise, at the time of purchase or creation of the assets. It becomes necessary to consider the vulnerability of the assets caused by different sources, for example, internal or external. The vulnerability may be identified within the following areas: ICT equipment, software or devices, personnel, organization, processes and procedures, management practices, physical environment, configuration of the information system, third party dependencies. The examples and assessment methods are presented in the tables below.

Table 4. Examples of vulnerability of the information resource XXX

Type of medium	Examples of vulnerability	Examples of threats
Electronic equipment	Unsecured devices for data storage	Theft of media or documents
	Lack of diligence when disposing of media	Theft of media or documents
	Uncontrolled copying	Theft of media or documents
Software	No logging out when leaving the workstation	Abuse of rights
	Use of application programs for outdated data	Data distortion
Personnel	Lack of monitoring mechanisms	Illegal data processing
	Work of third party personnel or cleaning staff without supervision	Theft of media or documents

The following table presents the examples of the vulnerability of the information resource, whose medium may be electrical equipment, software or a person.

Table 5. Example of assessment of vulnerability of the information resource XXX

Information asset: XXX Name of vulnerability of the resource	Expert's assessment 1	Expert's assessment 2	Expert's assessment 3	Expert's assessment 4	Expert's assessment 5	Average assessment of vulnerability
Unsecured devices for data storage	M	H	M	H	M	H
Lack of diligence when disposing of media	H	M	M	M	H	M
Uncontrolled copying	H	M	H	H	M	H
No logging out when leaving the workstation	H	M	M	M	H	M
Use of application programs for outdated data	H	M	H	H	M	H
Assessment of vulnerability of the information resource:						**H**

After the identification and vulnerability assessment process, the following is obtained:

1. List of vulnerability risks with respect to the assets, threats and security measures;
2. List of vulnerability risks, which do not refer to any identified threat, for the purpose of review; the vulnerability, with respect to which no relevant risk occurs, may not require implementation of the security measure, however, it is recommended to recognize it and monitor any changes with respect thereto.

The vulnerability may be related to the properties of the assets, which may be used in an intentional manner or otherwise, at the time of purchase or creation of the assets. It becomes necessary to consider the vulnerability

of the assets caused by different sources, for example, internal or external.

The examples of vulnerability and methods of assessment of vulnerability are in Appendix D, ISO 27005: 2013.

4 Estimation of risk/methods of estimation

The risk analysis may be conducted at different levels of detail, depending on the criticality of the assets, level of vulnerability and incidents, which the organization experienced in the past. Depending on the circumstances, the methodology of estimation may be qualitative, quantitative or mixed. In practice, the qualitative estimation is often applied first to obtain the general indication of the risk level and to disclose serious risks. Later on, it may be necessary to perform a more specific or quantitative analysis of such serious risks, since the qualitative analysis is usually less complex and cheaper than the quantitative analysis. Below you may find a more detailed description of the methodology of estimation.

4.1 Quantitative estimation

The quantitative estimation applies a numerical scale (contrary to the description scale used in the qualitative estimation) for both the consequences and probabilities, using the data from various sources. The quality of analysis depends on the accuracy and completeness of the figures as well as correctness of the used models. In the majority of cases, the quantitative estimation uses some historical data about the incidents, thanks to which the estimation may directly address the objectives of the information security and problems of a given organization. However, the lack of such data for new risks or vulnerability related to the information security may be considered a disadvantage. The disadvantage of the quantitative estimation may appear in the event, when the actual and verifiable data are not available, hence the illusion of value and accuracy of the risk assessment is created. The quantitative methods use numerical measures, such as specific amounts of the values of the IT resources, frequency of incidents or probability of their occurrence. One of the first methods was Courtney's method published in 1975, also known as the ALE (Annual Loss Exposure).

The ALE parameter is calculated based on the following formula:

$$ALE = SLE \cdot ARO \qquad (1)$$

where:
SLE (Single Loss Expectancy) – expressed in the currency, expected annual loss caused by a single incident,
ARO (Annualized Rate of Occurrence) – frequency of occurrence of an event causing loss.

SLE is expressed by the following formula:

$$ALE = AV \cdot RF \qquad (2)$$

where:
AV (Asset Value) – value of an asset
RF (Exposure Factor) – percentage of the value of an asset, which will be lost due to a single event.
In the course of the risk analysis by Courtney's method, the following formula is applied to calculate ARO for the purpose of simplification:

$$ALE = \frac{10^{f+i-3}}{3} \qquad (3)$$

where:
f – rate of occurrence
i - rate of loss value
The rate values are provided in table 6.

Table 6. Values of rates f and i

Rate i	Rate of occurrence	Rate f	Rate of loss
1	once per 300 years	1	$10
2	once per 30 years	2	$100
3	once per 3 years	3	$1000
4	once per 100 days	4	$10000
5	once per 10 days	5	$100000
6	once per day	6	$1000000
7	10 times per day	7	$10000000
8	100 times per day	8	$100000000

4.2 Qualitative estimation

The qualitative estimation uses qualitative attributes to describe the true scale of the potential consequences (e.g. low, medium and high) and the probability of their materialization. An advantage of this estimation is that it is easy to understand by practically all the competent employees, but it also depends on the subjective choice of the scale of attributes, which is a disadvantage. The scale may be adapted according to the circumstances, and, what is more, different descriptions may be applied to different types of risks. The qualitative estimation may be used as:

- initial review action (E.1) to identify the risks, which require a more detailed analysis (*General risk assessment concerning the information security*),
- basic action (E.2) to assess different variants of risk handling (*Detailed risk assessment concerning the information security)*.

It is recommended to use the available, actual data and information in the qualitative analysis.

E.1 General risk assessment concerning the information security

The general risk assessment allows to determine the priorities and sequence of actions. For various reasons, such as the budget, the implementation of all security measures at the same time may not be possible and only the most critical risks may be tackled during the risk handling procedure. Furthermore, it may be too early to start the detailed risk management if the management is anticipated in a year or two years time. The general risk assessment considers the business value of the

information assets and the risks related to the business activity of the organization. A number of factors allow to determine whether the general risk assessment is appropriate for handling the risk:

1. business objectives, which are to be achieved by using different information assets;
2. extent to which the business activity of the organization depends on particular information assets, i.e. whether the functions considered critical for the existence of the organizations or their efficient business operations depend on the said assets or confidentiality, integrity, availability, non-repudiation, accountability and reliability of the information of the information stored and processed by such assets;
3. investment expenses incurred with respect to particular information assets, in the field of development, maintenance or replacement of assets.
4. The information assets are the assets with the directly ascribed value by the organization.

Another reason for starting the general risk assessment is its synchronization with other plans related to the change management (or continued operation). For example, full protection of the organization, system or application is not rational in the event when they are to be outsourced in the nearest future. However, it may still be worthwhile to assess the risk for the purpose of an outsourcing agreement. The iteration properties of the general risk assessment may be the following:

1. The general risk assessment may refer to the overall picture of the organization and its information systems, including the technological aspects, independent of the business issues. Therefore, the contextual analysis may concentrate better on the business and operational environment instead of the technological elements.
2. The general risk assessment may refer to a more restricted list of threats and vulnerability risks grouped into the defined categories or, to speed up the process, it may focus on the risk or attack scenarios instead of their elements.
3. The risks recognized in the general risk assessment are often more general risk areas than particular, specifically defined risks. The handling of risk is then mainly directed at selecting common security measures applicable in the entire system.
4. However, the general risk assessment, due to the fact that it refers to technological details, is more appropriate for indicating organizational and non-technical security measures as well as technical or key management aspects or common technical security measures, such as back-up copies and anti-virus software.

The advantages of the general risk management are the following:

1. an introduction of a original, simple approach increases the chances to obtain approval of the risk assessment program.
2. a possibility of creating a strategic picture of the information security in the organization, i.e. efficient planning support.
3. It is possible to allocate the resources and finances there, where they would bring the highest profits, whereas the systems, which probably need protection the most, will be addressed in the first place.

Since the initial risk analyses are conducted on a high level, which is potentially less accurate, the only possible defect of such approach may be the fact that a part of the business process or systems may not be identified as needing the second, more detailed assessment. It may be avoided if the relevant information on all aspects of the organization and its information systems, including the data obtained on the basis of the incident assessment related to the information security, is provided. If such factors are assessed, the decision becomes easier. In the event when the objectives of the asset data are especially important for further business operations of the organization or if the assets face significant risk, it is recommended to perform another iteration, detailed risk assessment of the indicated information assets (or part thereof). The general rule to apply: if the lack of security of the information causes negative consequences for the organization, its business processes or assets, the second risk assessment iteration, at a more detailed level, is required for the purpose of identifying potential risks.

E.2 Detailed risk assessment concerning the information security

The detailed risk assessment process concerning the information security covers in-depth identification and evaluation of assets, assessment of threats for such assets and assessment of vulnerability. The results of such activities are later used for the risk assessment and identification of variants of handling the risk. The detailed activities usually require a lot of time, efforts and skills, therefore, they are more suitable for the high-risk information systems. Many methods use tables and combine the subjective and empirical measures. It is important for the organization to apply the method, which is the most convenient and reliable for the organization and which produces repeatable results. One of the methods/techniques based on tables is presented below.

Assumptions

Z1. The risk may be described by the following relations:

$$R : \mathrm{Z} \times \mathrm{P} \times S \to \mathrm{N} \tag{4}$$

where:

R - function of relations, defined as follows:

$$r(z, p, s) = n; z \in \mathrm{Z}, p \in \mathrm{P}, s \in S \tag{5}$$

Z ={L, M, H}; - a set of values reflecting the level of risk to a resource (a possibility of materialization of the risk): L- low risk level, M – medium risk level, H – high risk level;

P={L, M, H};- a set of values reflecting the criterion for easiness of use of the information resource by the risk (a level of vulnerability

of the resource, where: L- low use level, M – medium use level, H – high ruse level);

S={1, 2, 3, 4, 5, 6, 7, 8, 9,…};- a set of values reflecting a level of losses, in case of loss of the security attributes ascribed to the resource,

N - a set of numbers reflecting the risk measures on the adopted scale, e.g. from 1 to 13 for each combination.

Z2. Relations of R and the values of the risk measures are on the matrix - table 6, with the predefined values, in an organized way.

Table 7. Risk matrix - example

	Risk possibility	Low (L)			Medium (M)			High (H)		
	Easy use	L	M	H	L	M	H	L	M	H
Resource value (level of losses)	1	**1**	**2**	**3**	**2**	**3**	**4**	**3**	**4**	**5**
	2	**2**	**3**	**4**	**3**	**4**	**5**	**4**	**5**	**6**
	3	**3**	**4**	**5**	**4**	**5**	**6**	**5**	**6**	**7**
	4	**4**	**5**	**6**	**5**	**6**	**7**	**6**	**7**	**8**
	5	**5**	**6**	**7**	**6**	**7**	**8**	**7**	**8**	**9**
	6	**6**	**7**	**8**	**7**	**8**	**9**	**8**	**9**	**10**
	7	**7**	**8**	**9**	**8**	**9**	**10**	**9**	**10**	**11**
	8	**8**	**9**	**10**	**9**	**10**	**11**	**10**	**11**	**12**
	9	**9**	**10**	**11**	**10**	**11**	**12**	**11**	**12**	**13**

The colors in the above table have the meaning defined below:

- grey - area of acceptable risk,
- white - area of unacceptable risk,
- red - area of unacceptable risk of critical values.

Using these risk assessment methods, the current or suggested assets are evaluated in terms of replacement costs (i.e. quantitative measurements). The costs are then represented on the same qualitative scale as the scale used for the information resources of the information (see 3.1.). The applicable vulnerability and corresponding threats are considered for each type of assets. If there is vulnerability without a corresponding threat or a threat without corresponding vulnerability, currently, there is no risk (yet it is still recommended to monitor the changes of such situation). The correct line in the matrix is defined by the value of assets, and the correct column - by a possibility of materialization of a threat and easiness of use. For example, if the given assets have value 3, the risk is "high (H)" and vulnerability low "L", then the risk measure is 5. Let us assume that the given assets have value 2, e.g. for the purpose of modification, the level of risk is "low" and the easiness of use defined as high "H", then the risk measure is 4. The size of the matrix, from the point of view of the number of the risk probability category and the number of the asset evaluation category, may be adapted to the needs of the organization. Additional lines and columns may define, if necessary, additional risk measures. The advantage of such approach is the obtaining of the risk ranking, which should be addressed in the further steps.

5 Summary of the risk assessment process

In the risk assessment process, the following is defined:

1) value of the information assets,
2) identification of applicable risks,
3) existing (or potential) vulnerability,
4) identification of existing security measures and their impact on identified risk,
5) potential consequences,
6) indication of priorities of the obtained risks and their order in accordance with the criteria of risk assessment set during determined during the context setting.

The risk assessment is often performed in two (or more) iterations:

1) the first one consists in the general assessment performed to identify potentially high risks, which give a possibility of further assessment.
2) the second one covers subsequence, more detailed considerations regarding potentially high risks disclosed in the first iteration.

If it does not provide sufficient information for the risk assessment, a further, more detailed analysis is performed, presumably for the part of the entire scope and possibly using another method. The choice of the risk assessment approach, including the objectives of the risk assessment, depends on the organization.

Conclusions

The risk analysis and management (risk management system) constitute grounds for the management activities in the organization, aimed at minimizing the losses related to a critical situation or risk of the information security. It is a tool (element) supporting the indication of such area of activity of the organization, which should be verified and analyzed in the first place.

Regular and continuous risk analysis and management contribute to the improvement of efficiency and obtaining of consistent, comparable and reliable results. It should be remembered that the action-based approach to risk management may cause materialization of some serious undetected risks. Unfortunately, it is a difficult issue, which requires careful preparation and determination of a set of possible risk factors, building of awareness and proper merit-based approach of persons who analyze the risks in the security and quality management processes of the organization. It is necessary to apply the right approach, including comprehensive risk management in the organization, and not just risk assessment for some individual areas. At this point, it is important to analyze the basic rules of risk management in the context, whose application brings profits to the organization.

The risk analysis and management concerning the information security must be an integral part of the decision-making process, which contributes to the making of conscious and right choices, establishment of

priorities of activities and recognition of alternative directions of actions in case of the existing threats, events and critical situation. The correct risk analysis is based on the best practices and available sources of information, such as historical data, experiences, feedback information from all the interested parties, observations, forecasts and opinion of experts, including their variety and limitations, hence, it at the same time, contributes to the collection of data from many sources, including and explicitly defining a level of their uncertainty.

The risk analysis and assessment constitute the first element in the risk management process. The results of this process help to choose the right systems of security methods and to minimize or eliminate the identified risk factors. The risk management policy to a large extent depends on the nature of business, its approach and tendency to take risk, also known as the risk "appetite", and business environment. To support the process of introducing and maintaining efficient risk management, it is indispensable to work out a "common understanding" concerning the risks within the entire organizational unit and its environment. Without a common ground for discussion on the risks accompanying business operations of the organization, it is not possible to ensure powerful communication and introduce efficient risk management process within the entire organizational unit. It is also impossible if the subject concept is not understood in the same way by all employees of the organization. The risk is perceived in a different manner by the employees working on different levels of the organizational structure, responsible for particular business process (or located in different organization units of the same organization. The practical solution to find the "common understanding" concerning the risks within the entire organization is to use the standard valuation and risk assessment model.

References

1. T. Aven, *Risk assessment and risk management: Review of recent advances on their foundation*, European Journal of Operational Research, **253**: 1-13 (2016)
2. J. Aagedal, D. Braber, T. Dimitrakos, B. Gran, D.Raptis, K. Stolen, *Model-based risk assessment to improve enterprise security. In: Proceedings of the sixth international enterprise distributed object computing conference.* EDOC'02. 51–62, (2002)
3. F. Baiardi, C. Telmon, D. Sgandurra, *Hierarchical, model-based risk management of critical infrastructures*, Reliability Engineering and System Safety, **94**, 1403-1415 (2009)
4. A. Białas, *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, (WNT, 2007)
5. I. Eusgeld, C. Nan, S. Dietz., "*System-of-systems*" *approach for interdependent critical infrastructures, Reliability Engineering and System Safety*, **96**, 679-686 (2011)
6. K. Jajuga, *Zarządzanie ryzykiem*, (PWN, 2009)
7. A. Korczowski., *Zarządzanie ryzykiem w projektach informatycznych. Teoria i praktyka*, (Helion, 2013)
8. P. Matkowski, *Zarządzanie ryzykiem operacyjnym*, (Wolters Kluwer Polska, 2006)
9. J. Monkiewicz, L. Gąsiorkiewicz, *Zarządzanie ryzykiem działalności organizacji*, (Uczelnie Techniczne, 2010)
10. O. Patrick, *ISO 31000:2009 Risk management – Principles and guidelines* (2009)
11. J. Stanik, M. Kiedrowicz, *Selected aspects of risk management in respect of security of the document lifecycle management system with multiple levels of sensitivity*, Information Management in Practice, **18**, 231-251 (2015)
12. *PN ISO/IEC 27001 Information security management systems. Requirements*
13. *PN ISO/IEC 27005 Information technology. Security techniques. Information security risk management*
14. *PN-ISO 31000 Zarządzanie ryzykiem – Zasady i wytyczne*
15. *PKN–ISO GUIDE 73 Risk management - Terminology*
16. *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners*, NASA/SP-2011-3421, Sec.Ed. (2011)