Maciej Kiedrowicz*
Jerzy Stanik**

An information system risk model for the risk management system of an organisation processing sensitive data

Introduction

The awareness of risk and its potential consequences in organisations processing sensitive data (OPSD) forces the management of such organisations to continually analyse risk factors and areas and to adopt adequate security measures. When studying the usage of risk management system models or information system risk models in OPSDs, as well as risk management methodologies, one finds that no uniform, consistent, common procedure for ensuring sensitive data security and control has been developed so far and in particular – there has been no such procedure for an information system where documents representing different sensitivity levels are processed. Such projects have been implemented in this sector for several years now, but they still cannot be regarded as completed and perfect. Hence, the purpose of this study is to present a comprehensive model of the IT system risk. As the basic risk assessment tool, the model provides extensive and complete information for managing risk. The paper presents a systemic model of the IT system risk oriented towards security of sensitive data processing. The model represents a multi-dimensional approach to the IT system risk analysis and to information processes processed there. The presented approach addresses different categories of risk factors that follow for the IT system architecture, as well as information security elements and business continuity aspects. The model presented in the paper may become a starting point for developing a risk assessment method for IT systems, an adequate IT system security policy, which in turn, may provide inputs to an IT system risk management methodology.

The paper is a deliverable prepared under project no DOBR-BIO4/ /006/13143/2013 "An electronic lifecycle management system for documents representing different sensitivity levels" at the Military University of Technology in Warsaw.

* Dr inż., Wydział Cybernetyki, Wojskowa Akademia Techniczna, ul. Kaliskiego 2, 00-908 Warszawa, maciej.kiedrowicz@wat.edu.pl
** Dr inż., Wydział Cybernetyki, Wojskowa Akademia Techniczna, ul. Kaliskiego 2, 00-908 Warszawa, jerzy.stanik@wat.edu.pl

1. Sensitive documents, their risk sources and areas

The concept of a sensitive document has not been defined in legal terms, on the grounds of law. In the colloquial language, the term "sensitive data" is used. Hence, we shall be discussing documents that contain confidential information, not intended for an unlimited group of recipients, but for a narrow circle users, due to the nature of such information and the potential damage that may occur if it is disclosed. Documents representing different degrees of sensitivity include documents that require a special management approach. They may contain classified information, as well as information that needs special protection due to other aspects (e.g. bank documents). Such documents are usually handled in specially adapted areas, e.g. a secret registry (office) or an RFID[1] registry (office). Documents representing different levels of classifications are processed based on the current legislation and regulations that define the basic steps to be taken, resources and participants of these activities. A registry is the key actor of the document processing process. Inside any registry, many activities relating to the processing of various types of documents take place. As regards a secret registry (SR), documents representing different levels of classification are processed here. The most important publications include laws and regulations that constitute the primary source for research and analysis [Kiedrowicz, 2015; 2017].

The organisation/registry where sensitive documents are to be processed, needs to meet certain requirements that follow from legislation applicable to these issues. These requirements include: appointing a representative for the protection of classified information; establishing a security department within the organisation, to take responsibility for the processing of sensitive documents in the organisation; adapting the facilities so as to meet the legal requirements applicable to the production, processing, receipt, transmission, issue and protection of sensitive documents; arranging a secret registry; arranging a point (area, facility) for processing sensitive documents, including IT systems for the production and processing of sensitive documents [Kiedrowicz, Koszela, 2016].

The model of the risk management system of an organisation processing classified documents, as well as the processes that describe the principles

[1] RFID – radio-frequency identification – uses electromagnetic field to automatically identify and track tags attached to objects. The tags contain electronically stored information. Passive tags collect energy from a nearby RFID reader's interrogating radio waves. Active tags have a local power source such as a battery and may operate at hundreds of meters from the RFID reader [https://en.wikipedia.org/wiki/Radio-frequency_identification].

and methods of such an entity (e.g. a registry) operation were developed based on the legislation currently in force in Poland[2].

A special focus of this paper is on the IT system risk and the risk of processing sensitive documents, which has not been clearly defined yet either. For the purpose of IT consulting services, as well as for the purpose of this study, the risk of an IT system, as well as the risk of sensitive documents is defined as a threat that the information technology, the RIFD technology or other technologies related to the registry office activities and being used in the registry office (regardless its type and scale of activity):

- have not been implemented effectively and do not work as planned.
- prevent the implementation and improvement of a technical or technological infrastructure which supports risk management, in a manner that would be adequate to the current risk profile,
- do not ensure the acceptable level of the Registry and its resources security,
- do not meet such policy requirements as: security policy, quality policy, business continuity policy, etc.,
- do not ensure the adequate organisational structure as regards security forces,
- do not ensure that adequate documentation is kept as regards security, quality or business continuity,
- do not ensure the adequate integrity, confidentiality, undeniability and accessibility of sensitive data.

Considering the above, the risk of sensitive resources is analysed with the following categories and attributes covered (Fig. 1):

1) attributes in the field of information security: accessibility of sensitive documents, confidentiality of data processing, integrity of documents, compliance with security requirements specified in the security policy, losses understood as the cost of the loss of security attributes [Stanik et al., 2016];
2) elements in the area of legislation applicable to these security problems: appointing a representative for the protection of classified information; establishing a security department within the organisation, to take responsibility for the processing of sensitive documents in the organisation; adapting the facilities so as to meet the legal requirements applicable to the production, processing, receipt, transmission, issue and protection of sensitive documents; arranging a secret registry; arranging a point (area, facility) for processing

[2] The protection of classified Information Act dated 5 August 2010 (Journal of Laws 2010 No. 182, it. 1228).

sensitive documents, including ICT systems for the production and processing of sensitive documents;
3) basic quality and security related documents, such as: a risk analysis report, a security policy, an ICT security plan, special security requirements of an ICT system, safe operation procedures and a business continuity plan;
4) attributes/measures in the business process quality area: significance/relevance to the organisation and the client, compliance with the quality policy requirements;
5) attributes in the business continuity area: compliance with the security policy requirements applicable to process continuity, financial consequences of the process interruption/stoppage, cost and time of process inaccessibility;
6) in other areas: flexibility of sensitive documents processing, costs and duration of sensitive documents processing, effectiveness of change management, effectiveness of the sensitive documents processing architecture, reliability.

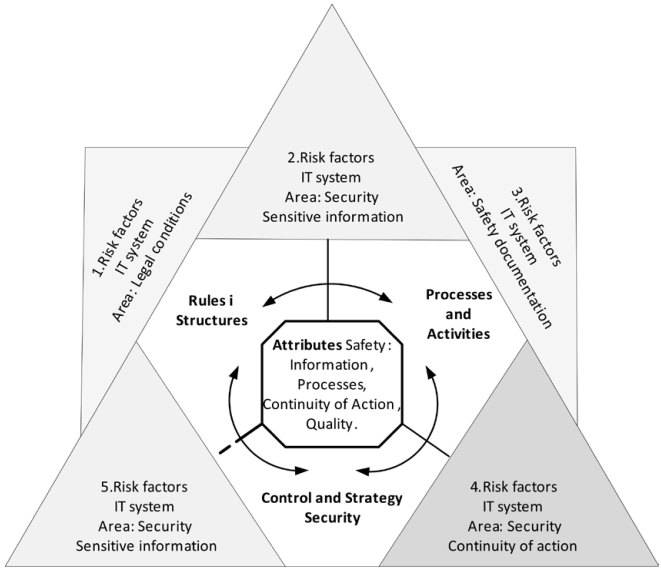
Finally, the following has to be emphasised:

1. Sensitive document security is the overall category of measures taken to secure data and information processed in an information or information and communication technology system against any unauthorised access, from their origination, throughout the period of use and distribution, up to the final disposal. A sensitive document is considered secure, if it has security attributes assigned to it [PN-ISO/IEC 27005, 2014].
2. Sensitive resource security is such a condition of the resource or its medium, where the risk of threats to the correct operation of the sensitive resource is reduced to an acceptable level.
3. Risk of a sensitive resource or of a process where sensitive data is processed can have such a seemingly trivial cause as an incorrectly designed IT system's user interface.
4. It is not possible to eliminate all risk from a registry office. Yet, some risk management systems include risk estimation methods [Bramlage, 1997], in particular – methods intended to estimate process risk or risks of systems where documents representing different sensitivity levels are processed, as well as risk reduction methods, these problems being the focus of this paper.

2. Main components of the sensitive resources risk and the risk of their processing

The information system security model of a registry office, presented in figure 1 is a starting point for designing an information system risk assessment model proposed in this paper, section 4: An information system risk model for the risk management system of a registry office, which reflects the systemic nature of the approach presented here.

Figure 1. Security model of a registry office information system where documents representing different levels of sensitivity are processed



Source: Own elaboration.

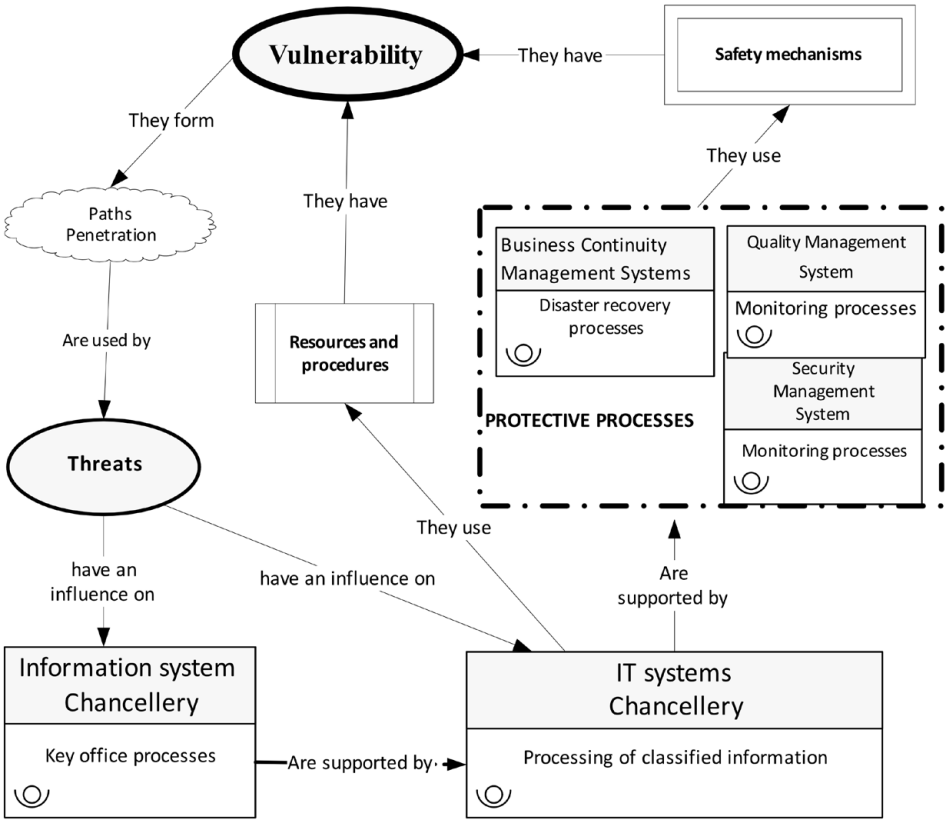
The model includes five perspectives and is based on the following three components:

Principles and structures. Principles – the strategy, policies and procedures that define the rules of ensuring sensitive information security, information processing and process continuity aspects; the implementation of these throughout the organisation determines the effectiveness of organisation management.

In the model presented in figure 1, principles include the following elements that determine the information IT systems risk level: the security policy, the security procedures, the business continuity plan (BCP), the disaster recovery plan (DRP). Of these, the security policy and the procedures ensuring safe operation of the information system are key determinants of the IT systems risk level.

1. Structures – a set of functions or structural units in the organisation, with their interfaces. The following structures are relevant to the purpose of this study: the risk management framework, the security function structure, the business continuity framework, the quality management function structure and the management control. The security function structure consists of: the head of the registry; the deputy head of the registry; the registry clerk; the security personnel that performs tasks related to the physical protection of sensitive information, including control of the access to area where classified information is processed; the ICT security inspector, the IT system administrator.
2. Processes and activities – the solutions that guarantee the correct operation of the organisation and ensure security of information processed there, quality [Stanik, Protasowicki, 2015], business continuity requirements and that are responsible for responding to any violations of policies and procedures, as well as to sensitive information security incidents. The category of Processes and Activities of the model presented in Figure 1 includes the following elements that may determine the level of IT systems risk: security processes, change management processes, control and safety processes. Figure 2 shows how security processes may influence the IT system risk, including in particular the processing of sensitive information.
3. Security control and strategy – monitoring the IT system operation and processing of documents representing different levels of sensitivity on a current basis, as well as verifying the compliance with security principles and the consistency and adequacy of these principles; solutions that guarantee the reduction of residual risk relative to the security attributes of sensitive information and resources or sensitive data processing and business continuity. Control is the last of the main components of the IT system security model. This component contains the following elements that can potentially influence the IT system risk level: the ICT environment complexity, the security monitoring system, the physical and logical access control and the human factor. The method of IT system risk analysis proposed in this study addresses all of these elements, but they are included in the method in different ways. The pillars of the model are interrelated in the following way:
   – the principles specified in the policies and procedures determine the functioning of security solutions and the methods of monitoring their operation,

Figure 2. Security processes in the information security management system of a registry office



Source: Own elaboration.

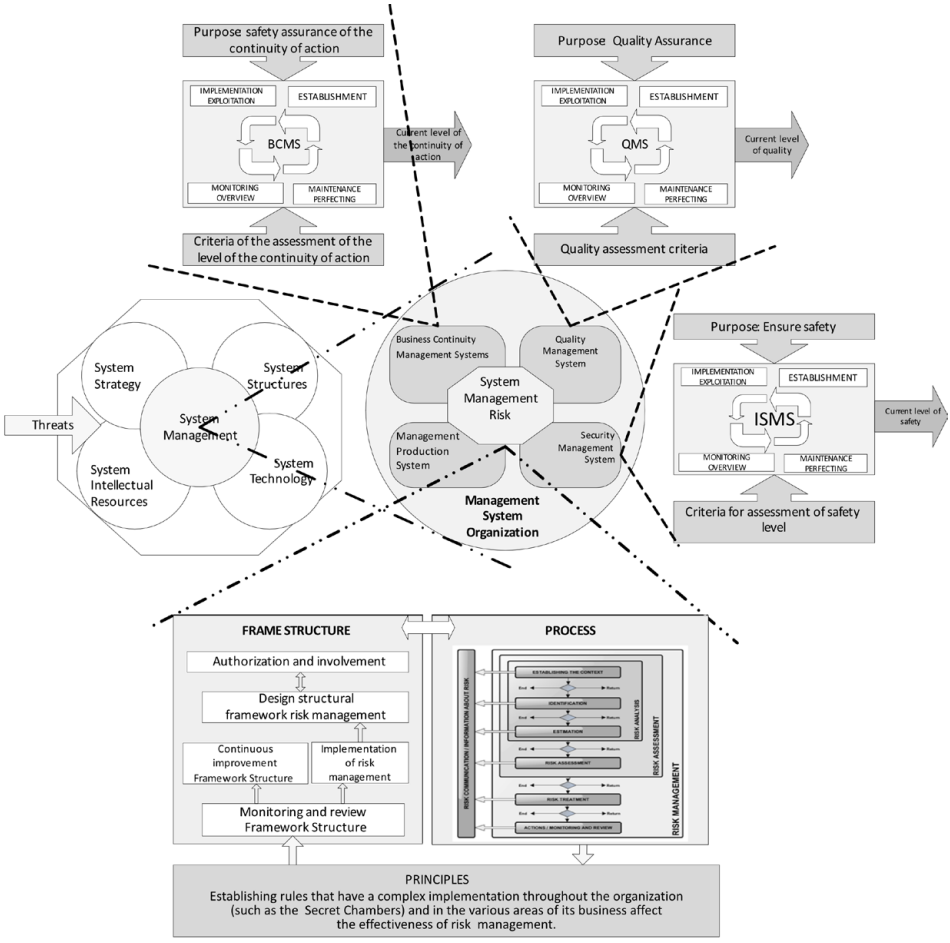
– security systems (solutions) functioning – determines the development of new security rules, determines the scope monitoring, business continuity and quality of processing,
– events detected owing to security monitoring determine modifications of security solutions – the security system, the information security management system and provide recommendations for the modification of existing security solutions, as well as for developing new security policies and procedures.

The so-defined model indicates the areas that determine the IT system risk, as well as ensures the completeness of approach, which has been proved in the course of wide practical application of the model. A set of the primary security attributes of an IT system is central to the IT system security model presented above.

3. The risk management system in the registry unit management system

Risk management system (RMS) – a set of principles, controls and tools (including policies and procedures for risk for identification, measuring, monitoring and treatment) referring to risk-related processes. The risk management system in a registry office cannot be detached from the corporate reality, but has to be an integral part of the organisation management (Fig. 3).

Figure 3. Risk Management System in the management system of an organisation



Source: Own elaboration.

The purpose of the risk management system is to identify, measure or estimate and monitor risks present in the registry operations, in order to ensure the correctness of setting and achieving goals of the registry

activity. The Management System should allow for a retrospective assessment of effectiveness of the registry actions taken in respect of: sensitive resources, sensitive resources processing, IT systems supporting the processing of sensitive data, registry personnel, technologies being used. The RMS consists of the following three elements: Risk Management Principles, Organisational Risk Management Framework, Risk Management Processes or Procedures. The implementation of both policy and procedures is preceded by evaluation of the organisation in terms of risk. A well-designed and implemented RMS enables categorisation of organisation's risks, supports the risk lifecycle and fully integrates with other systems in the organisation, e.g. the security management system, the business continuity management system and the quality management system (Fig. 3) [Hoffmann et al., 2016a; Hoffmann et al., 2016b].

4. The risk model concept

4.1. Definitions, terms and background

Let us accept the following terms and definitions for further considerations:

Def. 1. Process – P. A process is an organised sequence of steps taken to meet the needs of the process client. Fig. 1 presents the basic components of a process. It is a set of actions or activities aimed at achieving an expected result. The result is achieved through processing process inputs into process outputs. The processing is controlled by means of pre-defined rules. Fo the so-defined result to be achieved, adequate resources are needed.

Def. 2. Organisation – O. An organisation[3] is an intentionally established group of human and capital resources, where the primary functionality (a set of business activities and business processes) is supported by the use of dedicated IT systems and RFID technologies.

Def. 3. A set of processes for processing sensitive documents – P(O). A set of processes for processing sensitive documents is a finite and countable set of processes $P(O) = \{P_1, P_2, \ldots, P_i, \ldots, P_N\}$, where: N – is the number of processes for processing sensitive documents of O. An organisation is also defined as a "set of variable processes that remain in different relations of of mutual dependence". An organisation becomes a space where people are integrated around tasks and problems to be solved. Hence the need to merge different work contents, to combine tasks into processes and to develop the organisational structure in alignment with these

[3] In this paper, an organisation is a registry office using the RFID technology for tagging documents and controlling them within its capability and in accordance with the current legislation applicable to the processing of sensitive documents.

processes and not with centres of authority or functional specialisation [Sikorski, 1998].

Def. 4. Risk management process. According to international standards, a risk management process includes: risk assessment – including risk identification, analysis and evaluation, decision making, risk treatment, monitoring and review. This process applies to all risks and has to be an integral part of organization's activities in practice; it has to have an performer who is capable of ensuring adequate methods and tools for process implementation. Risk management is not limited to compiling a list of threats and actions taken. It requires a serious approach to risk assessment, which is a set of activities including but not limited to risk identification, analysis and evaluation. It is a system approach to the process, which required an adequately planned strategy.

For the purpose of designing the model presented in this paper, the risk of sensitive resources or of an IT system which supports the sensitive resources processing is defined as a threat, a vulnerability or a gap (e.g. in information, or in security), so that different types of technologies, e.g. IT, a designing or production technology used by the registry office (irrespective of its type and size):

- do not meet the organisation's strategy or policy requirements,
- do not ensure adequate quality or continuity of sensitive documents processing,
- do not ensure security monitoring on a current basis,
- are not monitoring the continuity of basic security attributes of sensitive resources, e.g. integrity, accessibility, confidentiality, etc.,
- have not been implemented effectively and do not work as planned or required by policies.

With regard to the above, the risk of a sensitive resource or of a process of sensitive resources processing is analysed in a breakdown by different categories [PN-ISO 31000, 2012], sources and areas:

1) the category of possible risk sources: natural and technical threats, imperfections (absence) of legislation, inappropriate behaviour patterns, human mentality, weakness of the organisation, insufficient training, low awareness of threats, no preparedness, unprepared personnel, absence of a system, security standards, quality standards and business continuity standards inadequate to reality, technical and technological development gaps, non-compliance with technological standards, mistaken actions, failure to act and negligence, ignorance, incompetence, (systemic) corruption,
2) the category of possible risk areas: processes, sensitive information, IT systems, environment in terms of security, quality and business

continuity, information and other unspecified elements, such as: an organisation, organisation's department or section,, natural environment, communities, etc.

The set of basic security attributes of a sensitive resource or of an IT system which supports sensitive data processing is decomposed into the following subsets/areas:

I. The information security area. This component includes the following security elements/attributes that can potentially affect the information resource/system risk level: confidentiality, sensitive data consistency, sensitive data accessibility, data undeniability. All of the information security attributes listed above are directly included in the risk model proposed in this paper.

II. The area of security of sensitive information processing continuity. This component includes the following elements that can potentially affect the information resource/system risk level: compliance with the process continuity policy requirements, Business Continuity Plan (BCP), Disaster Recovery Plan (DRP); financial consequences of the process discontinuity/stoppage, non-financial consequences of the process interruption/stoppage, cost and time of process unavailability;

III. The area of sensitive resources processing processes/areas security. This component includes the following elements that can potentially affect the information resource/system risk level:
   1. Availability of the process/system processing sensitive data – the property of being usable at a certain time, on request of an authorised actor in the registry office.
   2. Correctness of work/operation: Operating as expected by the registry office users.
   3. Process/system control: Controlling the access to the appropriate IT process/system.
   4. Audit: The resource/system can be endangered not only by unauthorised users. Those authorised often make mistakes, break the rules and even damage system elements deliberately. In a situation like this, one needs to check, what has been done, by whom and what are the consequences. The only way to obtain such information is to use a tamper-proof and damage-proof record in the system, which can identify the perpetrators and their actions. In some critical applications, certain operations can be undone, which may be helpful in restoring the system.

As far as security attributes of sensitive data processing processes/systems are concerned, the authors believe that a situation, where potential

lack of process or processed information integrity and continuity is tolerated cannot be accepted, therefore expectations with respect to each process/system integrity are comparable.

4.2. Components of the risk vector

The information system risk model for a registry office is defined as vector $\overrightarrow{R_{S_i}}$:

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

decomposed into three component vectors $\overrightarrow{R^B_{S_i}}$, $\overrightarrow{R^C_{S_i}}$, $\overrightarrow{R^T_{S_i}}$, which reflect the information system risk levels in the aspect of individual risk factor areas.

The risk vector coordinates represent different risk areas, each of which covers several risk factors, hereinafter referred to as the component vector constituents. Components of vector $\overrightarrow{R_{S_i}}$ used in the registry office information system risk model include":

I. With respect to the information security area – $R^B_{S_i}$:

1. Accessibility of data in the information system – λ_{S_i}. Accessibility of data in information system S_i is the property of being usable at a certain time, on request of an authorised actor in the registry office. The accessibility of data in the information system S_i is expressed by the fact of belonging to accessibility class $\lambda \in \Lambda$ and represented as λ_{P_i}.
2. Data confidentiality – α_{P_i}. Confidentiality of data of information system S_i is the property of not disclosing information to any parties that are not authorised to obtain it. Confidentiality of data processed by information system S_i is expressed by the fact of belonging to data confidentiality class $\alpha \in A$ and represented by α_{S_i}.
3. Compliance with the security policy requirements – $\eta^B_{S_i}$. A set of security policy requirements of organisation O is represented by a finite and countable set $W^B_{P(O)} = \{w_1, w_2, \ldots w_m, \ldots w_{M^B}\}$, where: M^B is the number of the security policy requirements with respect to P(O). For each of requirements $w_m \in W^B_{P(O)}$ the requirement priority value is defined with respect to information system S_i. Number $p^m_{S_i} \in \mathbb{N}$, is the priority of requirement $w_m \in W^B_{P(O)}$ with respect to information system S_i, where e.g.: 0 – means that the requirement is inadequate to information system S_i, 5 – means that the requirement is maximally relevant to information system S_i.
4. Performance of the security monitoring system – $\beta^B_{S_i}$, The performance of the security monitoring system for information system S_i is represented by polynominal

$$\beta^B_{S_i} = d^B_{SM}(S_i) \times \Sigma_j\left(\delta^m_{S_i} \times \upsilon^{k^j}_{S_i}\right); \quad (2)$$

where:
j – sequential number of the security monitoring system performance evaluation criterion,
$\delta_{S_i}^m$ – riority of the j-th criterion of the security monitoring system performance evaluation croterion S_i,
$\upsilon_{S_i}^{k^j}$ – value of the j-th criterion of the security monitoring system performance evaluation criterion S_i,
k^j – relevance of the j-th criterion of the security monitoring system performance evaluation criterion
$d_{SM}^B(S_i)$ – multiplier of the information system coverage S_i by the security monitoring system,

Where information system S_i is covered by different monitoring systems, the value of criteria for evaluating these monitoring systems performance should be determined.

II. With respect to the business continuity area – $R_{S_i}^C$:

1. Compliance with the business continuity policy requirements – $\eta_{S_i}^C$. The set of the business continuity policy requirements of organisation O is represented by finite and countable set $W_{P(O)}^C = \{w_1, w_2, \ldots w_m, \ldots w_{M^C}\}$, where: M^C is the number of the security policy requirements with respect to P(O). For each requirement $w_m \in W_{P(O)}^C$ the requirement priority value is defined with respect to information system S_i. The priority of requirement $w_m \in W_{P(O)}^C$ with respect to information system S_i is represented by number $p_{S_i}^m \in \mathbb{N}$.
2. Performance of the business continuity monitoring system – $\beta_{S_i}^C$. The performance of the business continuity monitoring system for information system S_i, similarly as in case of security monitoring, is represented by polynominal:
$$\beta_{S_i}^C = d_{SM}^C(S_i) \times \Sigma_j\left(\delta_{S_i}^m \times \upsilon_{S_i}^{k^j}\right). \quad (3)$$
3. Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP). The model proposed in this paper does not include the BCP or DRP evaluation. The reason is that issues related to BCP are associated with business risks rather than with information systems risks, while DRP is directly related to the attribute of information systems accessibility.
4. Cost of information system inaccessibility – κ_{S_i}. The cost of information system inaccessibility includes all costs related to performing the bundle of operations the information process consists of (Fig. 1). For the purpose of estimating the cost of information system inaccessibility, an assumption is made that an event causing an interruption to information processing will occur at the worst moment. The cost of inaccessibility of information system S_i is the property,

which is a measure consisting of financial consequences of process interruption and non-financial consequences of process interruption. The cost of process inaccessibility is expressed by the process attribution to the class of inaccessibility costs $\kappa \in K$ and represented as κ_{S_i}.

5. Maximum time of the sensitive information processing inaccessibility – π_{S_i}. The maximum time of process inaccessibility is the time, when its operation has to be restored, so as to prevent any significant financial or non-financial consequences. The maximum time of process inaccessibility is expressed by the process attribution to the class of inaccessibility costs $\pi \in \Psi$ and represented as π_{S_i}.

III. With respect to the area of sensitive information processing security – $R_{S_i}^T$:

1. Compliance with the process security policy requirements – $\eta_{S_i}^T$. The set of security policy requirements for the processing processes of organisation O is represented by a finite and computable set $W_{P(O)}^T = \{w_1, w_2, \ldots w_m, \ldots w_{M^T}\}$, where: M^T is the number of the security policy requirements with respect to processing processes $P_j \in S_i \in P(O)$. For each requirement $w_m \in W_{P(O)}^T$ the requirement priority value is defined with respect to IT system S_i. The compliance with requirement $w_m \in W_{P(O)}^T$ with respect to IT system S_i is represented by number, $s_{S_i}^m \in [0\%, \ldots, 100\%]$.
2. Quality monitoring system performance – $\beta_{S_i}^T$. The performance of quality monitoring for IT system S_i is represented by polynominal $\beta_{S_i}^T = d_{SM}^T(S_i) \times \Sigma_j\left(\delta_{S_i}^m \times \upsilon_{S_i}^{k^j}\right)$.
3. Duration of the process of information processing – δ_{S_i}. This is the average duration of all information processing operations. The duration of processing depends first of all on the level on which procedures are organised, as well as on the level of obtaining the added value. The duration of sensitive information processing is expressed by the attribution of the process to processing duration class $\delta \in \Delta$ and represented as δ_{S_i}.
4. Information system flexibility – ϑ_{S_i}. The flexibility of information system S_i is the capability of the system to change, improve, change the sequence of operations, merge operations, etc. The flexibility of information system S_i is also determined by its susceptibility to transformation of resources that have been used, as well as by the promptness of change in response to customer's request. The flexibility of information system S_i is expressed by the fact of belonging to flexibility class $\vartheta \in \Theta$ and represented by ϑ_{S_i}.
5. Information system relevance – ζ_{S_i}. The relevance of information system S_i is the property which is the measure consisting of the level

of recipient satisfaction and customer satisfaction, the level of revenue generated by the system and the level reflecting the strength of relationship between the system and the client. The relevance of information system S_i is expressed by the fact of belonging to relevance class $\zeta \in Z$ and represented as ζ_{S_i}. Each element of information system $S_i \in P(O)$, $i \in \{1, 2, \ldots Z\}$, belongs to one and only one class of information system relevance $\zeta \in Z$.

6. Change management process performance – φ_{S_i}. The performance of the change management process is the level of the organisation's change management process compliance with respect to its information system S_i, with the best practices in this field. The performance of the change management process with respect to information system S_i is expressed by the percent of compliance of the change management process existing for information system S_i with the relevant recommendations of the ITIL standard [Geddes, Ratcliffe, 2002].

4.3. Normalized components if the information system risk vector

Due to the fact that the co-ordinates of the information system's risk vector and the risk factors within the areas discussed belong to different sets of values, it is necessary to introduce function ξ or a set of functions $\xi \in \Xi$ that map these components into a uniform interval of values. The normalization function is represented by the family of functions $\xi: X \longrightarrow [1, 2, \ldots, N]$. The forms of normalization function from family Ξ should be defined in such a manner that their values are mapped into interval [1,..., N][4], and that the proportions of their effect on the information system's total risk are retained properly, with set X of all risk factors specified taken into account, decomposed into subsets X^B, X^C, X^T that represent the areas aspects of sensitive data processing security, quality and continuity. With the above assumptions and limitations taken into account, normalization functions $\xi \in \Xi$ look as follows (Table 1):

[4] Further in this paper, interval [1, ..., 24]. is used. The intention is to obtain the simplest shape of the functions mapping the model components (see Table 1) into a uniform range of values, while ensuring the legibility of the risk analysis results.

Table 1. Examples of normalization functions

A. For function $\xi \in \Xi^{B}$	accessibility $\xi_{\lambda}(\lambda_{S_i}) =$	data confidentiality $\xi_{\alpha}(\alpha_{S_i}) =$	compliance with requirements PB $\xi_{\eta}^{B}(\eta_{S_i}^{B}) =$	security monitoring $\xi_{\eta}^{B}(\beta_{S_i}^{B}) =$
Normalization function	$\begin{cases} 1, \text{ when } \lambda_{S_i} = \text{V} \\ 7, \text{ when } \lambda_{S_i} = \text{IV} \\ 13, \text{ when } \lambda_{S_i} = \text{III} \\ 19, \text{ when } \lambda_{S_i} = \text{II} \\ 24, \text{ when } \lambda_{S_i} = \text{I} \end{cases}$	$\begin{cases} 1, \text{ when } \alpha_{S_i} = \text{E} \\ 7, \text{ when } \alpha_{S_i} = \text{D} \\ 13, \text{ when } \alpha_{S_i} = \text{C} \\ 19, \text{ when } \alpha_{S_i} = \text{D} \\ 24, \text{ when } \alpha_{S_i} = \text{A} \end{cases}$	$1 + 23 \times \left(1 - \frac{\eta_{S_i}^{B}}{100\%}\right)$	$24 - \sqrt[2]{\frac{\beta_{P_i}^{C}}{2}}$
B. For function $\xi \in \Xi^{C}$	cost of inaccessibility $\xi_{\kappa}(\kappa_{S_i}) =$	maximum inaccessibility time $\xi_{\pi}(\pi_{S_i}) =$	compliance with requirements of PC $\xi_{\eta}^{C}(\eta_{S_i}^{C}) =$	continuity monitoring $\xi_{\eta}^{C}(\beta_{S_i}^{C}) =$
Normalization function	$\begin{cases} 1, \text{ when } \kappa_{S_i} = \text{V} \\ 7, \text{ when } \kappa_{S_i} = \text{IV} \\ 13, \text{ when } \kappa_{S_i} = \text{III} \\ 19, \text{ when } \kappa_{S_i} = \text{II} \\ 24, \text{ when } \kappa_{S_i} = \text{I} \end{cases}$	$\begin{cases} 1, \text{ when } \pi_{S_i} = 4 \\ 7, \text{ when } \pi_{S_i} = 3 \\ 13, \text{ when } \pi_{S_i} = 2 \\ 19, \text{ when } \pi_{S_i} = 1 \\ 24, \text{ when } \pi_{S_i} = 0 \end{cases}$	$1 + 23 \times \left(1 - \frac{\eta_{S_i}^{C}}{100\%}\right)$	$24 - \sqrt[2]{\frac{\beta_{P_i}^{C}}{2}}$
C. For function $\xi \in \Xi^{T}$	system relevance $\xi_{\zeta}(\zeta_{S_i}) =$	system flexibility $\xi_{\vartheta}(\vartheta_{S_i}) =$	compliance with quality Policy requirements $\xi_{\eta}^{T}(\eta_{S_i}^{T}) =$	quality monitoring $\xi_{\eta}^{T}(\beta_{S_i}^{T}) =$
Normalization function	$\begin{cases} 1, \text{ when } \zeta_{S_i} = \text{VI} \\ 7, \text{ when } \zeta_{S_i} = \text{V} \\ 13, \text{ when } \zeta_{S_i} = \text{IV} \\ 16, \text{ when } \zeta_{S_i} = \text{III} \\ 20, \text{ when } \zeta_{S_i} = \text{II} \\ 24, \text{ when } \zeta_{S_i} = \text{I} \end{cases}$	$\begin{cases} 1, \text{ when } \vartheta_{S_i} = 4 \\ 7, \text{ when } \vartheta_{S_i} = 3 \\ 13, \text{ when } \vartheta_{S_i} = 2 \\ 19, \text{ when } \vartheta_{S_i} = 1 \\ 24, \text{ when } \vartheta_{S_i} = 0 \end{cases}$	$1 + 23 \times \left(1 - \frac{\eta_{S_i}^{T}}{100\%}\right)$	$24 - \sqrt[2]{\frac{\beta_{S_i}^{T}}{2}}$

Source: Own elaboration.

The form of normalization functions from family Ξ presented in the table above is defined in a manner so as to map their value onto adequate intervals and to retain adequate proportions of their effect on the information system's risk.

4.4. The information system risk vector

As the information system risk model, vector $\overrightarrow{R_{P_i}}$ is taken and defined as follows:

$$\overrightarrow{R_{S_i}} = \langle \overrightarrow{R^B_{S_i}}, \overrightarrow{R^C_{S_i}}, \overrightarrow{R^T_{S_i}} \rangle \in M_{m\times n} \times M_{m\times n} \times M_{m\times n} \tag{4}$$

where:

- $M_{m\times n}$ – a matrix with dimensions m×n; as square matrixes 2×2 are used in this paper, m = 2 and n = 2,
- $\overrightarrow{R^B_{S_i}}$ – co-ordinates of vector $\overrightarrow{R_{S_i}}$ which characterizes the information security aspect of IT system S_i, and is a linear combination of risk elements of IT system S_i in the base of linear space $(M_{2\times2}, R, +, \cdot)$.
- $\overrightarrow{R^C_{S_i}}$ – a co-ordinate of vector $\overrightarrow{R_{S_i}}$ which characterizes the continuity aspect of IT system S_i, and is a linear combination of risk elements of IT system S_i in the base of linear space $(M_{2\times2}, R, +, \cdot)$.
- $\overrightarrow{R^T_{S_i}}$ – a co-ordinate of vector $\overrightarrow{R_{S_i}}$ which characterizes the security of sensitive information processing in IT system S_i, and is a linear combination of risk elements of IT system S_i in the base of linear space $(M_{2\times3}, R, +, \cdot)$..

$(M_{m\times n}, R, +, \cdot)$ – vector space defined as a set of matrices $M^{m\times n}$ with matrix addition vector + i and external operator · is a vector space over the field of real numbers, and:

$$\begin{aligned}
\overrightarrow{R^B_{S_i}} &= \xi_\lambda(\lambda_{S_i}) \cdot \vec{\lambda} + \xi_\alpha(\alpha_{S_i}) \cdot \vec{\alpha} + \xi^B_\eta(\eta^B_{S_i}) \cdot \overrightarrow{\eta^B} + \xi^B_\beta(\beta^B_{S_i}) \cdot \overrightarrow{\beta^B} \\
\overrightarrow{R^C_{S_i}} &= \xi^C_\eta(\eta^C_{P_i}) \cdot \overrightarrow{\eta^C} + \xi^C_\beta(\beta^C_{P_i}) \cdot \overrightarrow{\beta^C} + \xi_\kappa(\kappa_{P_i}) \cdot \vec{\kappa} + \xi_\pi(\pi_{P_i}) \cdot \vec{\pi}, \\
\overrightarrow{R^T_{S_i}} &= \xi^T_\eta(\eta^T_{P_i}) \cdot \overrightarrow{\eta^T} + \xi^T_\beta(\beta^T_{P_i}) \cdot \overrightarrow{\beta^T} + \xi_\vartheta(\vartheta_{S_i}) \cdot \vec{\vartheta} + \xi_\zeta(\zeta_{S_i}) \cdot \vec{\zeta},
\end{aligned} \tag{5}$$

where: $\vec{\lambda}$, $\vec{\alpha}$, $\overrightarrow{\eta^B}$, $\overrightarrow{\eta^C}$, $\overrightarrow{\eta^T}$, $\overrightarrow{\beta^B}$, $\overrightarrow{\beta^C}$, $\overrightarrow{\beta^T}$, $\vec{\kappa}$, $\vec{\pi}$, $\vec{\vartheta}$, $\vec{\zeta}$ – base vectors of vector space $(M_{2\times2}, R, +, \cdot)$ from algebra $(M_{m\times n}, R, +, \cdot, \otimes)$. Since the dimension of algebra $(M_{2\times2}, R, +, \cdot, \otimes)$ equals [Trajdos, 1993]: dim $(M_{2\times2}, R, +, \cdot, \otimes) = 4$ hence, to define component vectors $\left(\overrightarrow{R^B_{S_i}}, \overrightarrow{R^C_{S_i}}, \overrightarrow{R^T_{S_i}}\right)$ there are 12 base vectors defined as follows:

$$\begin{aligned}
&\vec{\lambda} = \begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}; \quad \vec{\alpha} = \begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}; \quad \overrightarrow{\eta^B} = \begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}; \quad \overrightarrow{\eta^C} = \begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}; \\
&\overrightarrow{\eta^T} = \begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}; \quad \vec{\zeta} = \begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}; \quad \overrightarrow{\beta^B} = \begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}; \quad \overrightarrow{\beta^C} = \begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}; \\
&\overrightarrow{\beta^T} = \begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}; \quad \vec{\kappa} = \begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}; \quad \vec{\pi} = \begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}; \quad \vec{\vartheta} = \begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix};
\end{aligned} \tag{6}$$

The linear combination of the above formulas shows that the impact of all dimensions/factors of the IT system risk analysis on each individual co-ordinate $\left(\overrightarrow{R^B_{S_i}}, \overrightarrow{R^C_{S_i}}, \overrightarrow{R^T_{S_i}}\right)$ of risk vector $\overrightarrow{R_{S_i}}$ is the same In order to estimate the IT system risk level more precisely, it may be necessary to assign to each of the vector co-ordinates, as well as to risk components, weighs of their effect on the final level of the IT system risk and to modify the co-ordinates of risk vector $\overrightarrow{R_{P_i}} \in M_{m\times n} \times M_{m\times n} \times M_{m\times n}$ using these weighs of effect. This problem is not discussed in this article.

4.5. The information system risk level

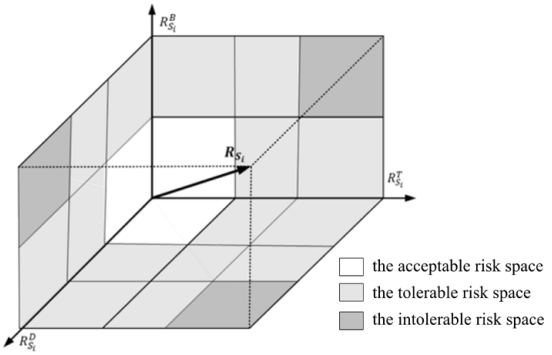
Having defined the concept of information system risk vector and defined its co-ordinates in algebra $(M_{m\times n}, R, +, , \otimes)$, wishing to determine the total risk level for information system S_i one needs to determine values $R^B_{S_i}; R^C_{S_i}; R^T_{S_i}$ first and next – value R_{S_i}. The risk of co-ordinate $\left(\overrightarrow{R^B_{S_i}}, \overrightarrow{R^C_{S_i}}, \overrightarrow{R^T_{S_i}}\right)$ of vector $\overrightarrow{R_{S_i}}$ of information system S_i in algebra $(M_{2\times 2}, R, +, , \otimes)$ is represented by number $R^B_{S_i}; R^C_{S_i}; R^T_{S_i} \in \mathcal{R}$ which equals the length of the vector, i.e.:

$$R^B_{S_i} = \left\|\overrightarrow{R^B_{S_i}}\right\|^5; R^C_{S_i} = \left\|\overrightarrow{R^C_{S_i}}\right\|; R^T_{S_i} = \left\|\overrightarrow{R^T_{S_i}}\right\| \tag{7}$$

Values $R^B_{S_i}; R^C_{S_i}; R^T_{S_i} \in \mathcal{R}$ quantify risk components of information system S_i. In order to present the level of risk for each co-ordinate of vector $\overrightarrow{R_{S_i}}$ qualitatively, appropriate risk intervals have to be used. The information system risk level can be determined as a module of vector $\left|\overrightarrow{R_{S_i}}\right|$ (Fig. 4.):

$$\overrightarrow{R_{S_i}} = \left|\overrightarrow{R_{S_i}}\right| = \sqrt[2]{R^{B\,2}_{S_i} + R^{C\,2}_{S_i} + R^{T\,2}_{S_i}}, \tag{8}$$

Figure 4. Vector $\overrightarrow{R_{S_i}}$ of the information system risk in the co-ordinate system $R^B_{S_i}; R^C_{S_i}; R^T_{S_i}$.



Source: Own elaboration.

[5] The length of vector $\vec{A}=[a_{ij}]$ equals $\left\|\vec{A}\right\| = \sqrt{\Sigma_i \Sigma_j a^2_{ij}}$.

Below, an example of a key for the evaluation of risk significance $R^{B}_{S_i}$ is presented [Szczepankiewicz, Wójtowicz, 2015]:

- acceptable risk (1–16 points) a low level of risk, which may cause short-lived, minor interruptions to the organisation processing sensitive data (OPSD), represents the lowest threat to the achievement of OPSD's goals and objectives; no additional activities are required to prevent risk; risk is subject to monitoring and control; risk controls are implemented;
- conditionally acceptable risk (17–36 points) a low level of risk, which causes medium interruptions to the OPSD operation; requires monitoring and some actions intended to minimize risk, its probability and/or consequences;
- serious risk (37–60 points) a high level of risk, which causes interruptions to the OPSD operations, requires special monitoring; may require additional controls or new internal regulations, as well as risk treatment actions intended to reduce risk to an acceptable level;
- critical risk (61–100 points) a very high level of risk, which is characterised by a high probability of materialising; it represents the greatest threat to the achievement of the OPSD's goals and objectives; requires unquestionably that additional actions are taken to minimise its probability or consequences, risk treatment methods are developed and security controls and monitoring are implemented.

Conclusions

Considering the diversity of factors and the wide range of their impacts on sensitive information processing, risk analysis should be an inseparable element of any risk management system, decision-making processes and the planning of operating variants in any registry office. The understanding of risks present in the process of sensitive information processing enables organisations to develop this process in such a manner that security reaches an acceptable level (Fig. 4). When analysing the sources and categories of risk in sensitive information processing, one should first of all focus on the characteristics of these processes, the IT system architecture and its lifecycle. This knowledge, supported by security statistics and statistics of the sensitive information processing system architecture, seems to be the key to the minimizing of risk in all its aspects – human, environmental, security, quality and economy. The considerations presented in this paper are mainly cognitive in their nature, hence no formal description of some problems has included. The authors' intention was to present a concept of an approach to threat quantification, which is different from traditional perspectives. The risk model of a registry office IT system where sensitive

information is processed, is characterised by a high complexity, which is a result of using the mathematical apparatus. Due to this complexity, caused by the fact that many factors affecting the IT system's risk level, as well as many processes of the system have been included, it is practically impossible to determine the risk of sensitive information processing in a correct, time and cost-effective manner and to manage this risk using traditional methods, without information technology solutions or computer techniques.

References

Bramlage J. (1997), *A new paradigm for performing risk assessment*, Computer Associates International, Inc., Reston VA.

Geddes G., Ratcliffe D. (2002), *ITIL Process Maturity Self–Assessment & Action Plan*, Pink Elephant Inc.

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

Hoffmann R., Kiedrowicz M., Stanik J. (2016b), *Risk management system as the basic paradigm of the information security management system in an organization*, „MATEC Web of Conferences", Vol. 76, 20th International Conference on Circuits, Systems, Communications and Computers (CSCC 2016).

Kiedrowicz M. (red.) (2015), *Zarządzanie informacjami wrażliwymi. Wybrane aspekty organizacyjne, prawne i techniczne ochrony informacji niejawnych*, WAT, Warszawa.

Kiedrowicz M. (red.) (2017), *Zarządzanie informacjami wrażliwymi. Otoczenie systemu, elementy i implementacja*, WAT, Warszawa,

Kiedrowicz M., Koszela J. (2016), *Modelowanie procesów biznesowych przetwarzania dokumentów wrażliwych z wykorzystaniem technologii RFID*, "Roczniki Kolegium Analiz Ekonomicznych", nr 42, SGH, Warszawa.

ISO/IEC 27005 (2014), Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji.

PN-ISO 31000 (2012), Zarządzanie ryzykiem.

Sikorski Cz. (1998), *Projektowanie i rozwój organizacji instytucji*, Polskie Wydawnictwo Ekonomiczne, Warszawa.

Stanik J., Napiórkowski J., Hoffmann R. (2016), *Zarządzanie ryzykiem w systemie zarządzania bezpieczeństwem organizacji*, "Zeszyty Naukowe Uniwersytetu Szczecińskiego, Ekonomiczne Problemy Usług", nr 123, Szczecin.

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

Szczepankiewicz E., Wójtowicz A. (2015), *Model rejestru ryzyka w jednostkach sektora finansów publicznych*, "Zeszyty Naukowe Uniwersytetu Szczecińskiego" nr 864, "Finanse, Rynki Finansowe, Ubezpieczenia", nr 76.

Trajdos T. (1993), *Matematyka*, Wydawnictwa Naukowo-Techniczne, Warszawa.

An information system risk model for the risk management system of an organisation processing sensitive data (Summary)

Objective – the focus of the paper is on the risk model of an information system where documents representing different sensitivity levels are processed in offices where IT systems and RIFD technologies are used. The model represents a multi-dimensional approach to the IT system risk analysis and to information processes processed there. *Research methodology* – the following methods were used: a review of the literature and of applicable legislation, a critical analysis of the analysed organisation's sensitive resources. *Outcome* – the article presents a risk model and examples of risk factors related to the threats present in different phases of an IT system lifecycle, presented in manner enabling a possibly complete and explicit determination of the risk level, while retaining practical utility of the approach. *Original value* – the paper seeks an answer to the question: "is it possible to design a comprehensive and adequate risk assessment model for an information system, where resources representing different sensitivity levels are processed?" The model proposed in the paper has been used for developing a framework structure of a risk management system and an information system security policy for the organisation where a risk assessment exercise was performed using the model.

Keywords
risk, risk model, risk analysis, risk management system, sensitive data