Theoretical and Applied Informatics
ISSN 1896-5334
Vol. 26 (2014), no. 3, 4
pp. 119 - 135

Internal control standards and software support for risk management in public administration

Jacek BAGIŃSKI[a]

[a] Instytut Technik Innowacyjnych EMAG
ul. Leopolda 31, Katowice, Poland
jbaginski@emag.pl

Abstract: The chapter deals with the issue of the risk and security management process in public administration, according to the internal audit standards and their requirements. Main legal acts and standards were specified and shortly described. Specially the risk analysis process and security measures selection were emphasized. The possibility to use the software tools for the risk analysis and security measures selection support in public administration was presented. The experiment of OSCAD usage in public administration was shortly described and its results were presented. This experiment shows that the software primarily intended for IT Security Management can be used for risk management in different area as well, for example – in public administration. Some possibilities of further development of risk management supporting tools were proposed

Keywords: risk management, risk analysis, software support, internal control standards, information security, business continuity

1. Introduction

Until recently IT systems security was a domain which required only good technical skills.

The Act of 29 August 1997 on the Protection of Personal Data [1] and its executive provisions specify only a set of IT security requirements, for example basic technical and organisational conditions which should be fulfilled by devices and computer systems used for personal data processing. Different IT security requirements are specified in the document, depending on the needed level of protection. The list of requirements contains, among others, the following technical issues:

- physical protection of data processing,
- access control to computer systems,
- backups preparation,
- data storage devices usage and disposal.

"The confidential data protection act" [2] contains similar set of security requirements for IT systems used for the classified information processing.

These legal regulations give some requirements without specifying the way of their implementation. The same requirements can be fulfilled with the use of different software or hardware solutions. Network separation can be solved by physical or logical network segmentation. Data privacy can be preserved using cryptographic software or hardware modules. For example cryptographic keys can be stored in operating system stores saved on the same disk as the system itself. Hardware security modules (HSM) can be used too. Commercial or free solutions (e.g. functions built in an operating system) can be used to control users' access and users' activities.

Thus nowadays, IT security officers should be also good managers which will ensure that a selected security measure will reduce existing risks to an acceptable level and its implementation will be justified from the business and financial points of view.

The obligation of such approach and inclusion of risk analysis and risk management and security measures selection comes from new legal regulations in European and Polish public administration. Those regulations relate to all public administration units and state-owned institutions where such issues as risk management were not always properly addressed and implemented. An important issue is how to prepare security officers in public administration units to fulfill new roles of analysts and managers, and how to support them with software tools.

Similarities of different management systems, like risk analyses elements, monitoring and review (including effectiveness measurement), enable to use the same supporting software tools dedicated to different standards.

As presented in Fig. 1, the basis of each management system are common requirements, which can be supplemented with specific requirements of different systems (depending on the institution's needs) and integrated into one, common management system.

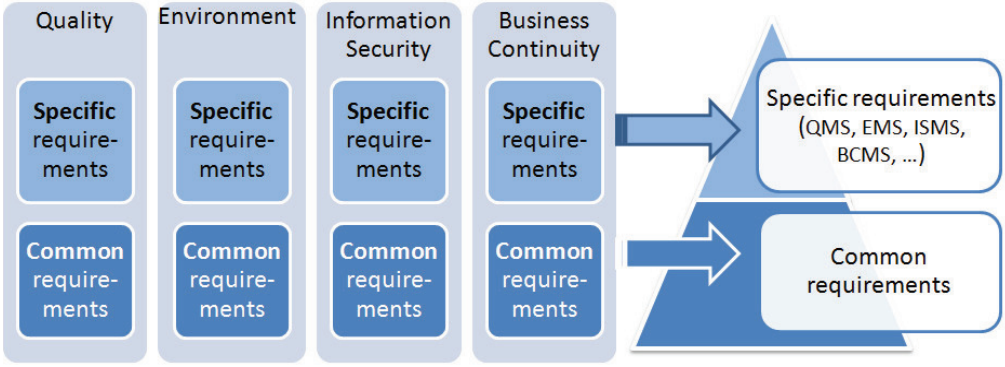

Fig. 1. Common and specific requirements integrated into one management system [13]

The article presents the results of experiment which shows that, the software primarily intended for different management system (e.g. IT Security Management)

can be used in different area (in this case – public administration), as a support of different elements of management process (e.g. for risk management activities).

To prove this assumption, the internal control process and related main legal acts and standards were identified and their requirements were analyzed. Based on this analysis, common elements of these standards and existing software tools could be found, and selected tool could be configured to check if it properly supports selected elements of the internal control process.

2. Main legal acts for risk management in public administration

In 2009, the Polish Finance Ministry published a regulation [3] which enforces the requirement of risk management implementation for the public finance sector. The requirement of Internal Control Standards implementation directly comes out of the EU framework [4] and includes guidelines described in [5]. Based on this guideline and other documents pointed in these framework, Polish governmental units, such as the Council of Ministers or Ministry of Finance, issued a set of regulations which take into consideration risk management and risk analysis as well as security aspects within the holistic management process. Since the requirements in the regulations were not clearly specified, three years later different guidelines related to these aspects were published (also by the ministries, e.g. [6]) to improve and support the implementation of risk and security management and security measures selection.

Requirements for the management of the information security occur in the regulation published in 2012 by the Polish Council of Ministries and called the regulation for the National Frames of Interoperability for public registers and electronic data exchange [7]. This document relates, among others, to information security in public administration. The requirements in chapter IV of this document are directly based on the ISO 27001 standard and its appendix A [8]. In most cases the requirements in the legal acts are based on general statements specified in security management standards which describe the requirements of Information Security Management Systems (ISO 27001) or Business Continuity Management Systems (ISO 22301[9]).

The risk management process has already been well defined in international standards, like ISO 31000 [10], ISO 31010 [11], and ISO 27005 [12]. The latter belongs to the ISO 27000 set of standards, related to the Information Security Management Systems. ISO 27005 specifies in details the requirements and good practices for risk management as a part of the ISMS. Chapters 7, 8 and 9 of the internal audit control regulation [3] include statements based on the mentioned risk management standards.

These regulations and standards rely on the same organizational basis. Thus the analysis was performed to list similarities between the Internal Control Standards (ICS) and different management systems.

A properly implemented risk management process should consist of a number of activities (Fig. 2) common for different management systems.

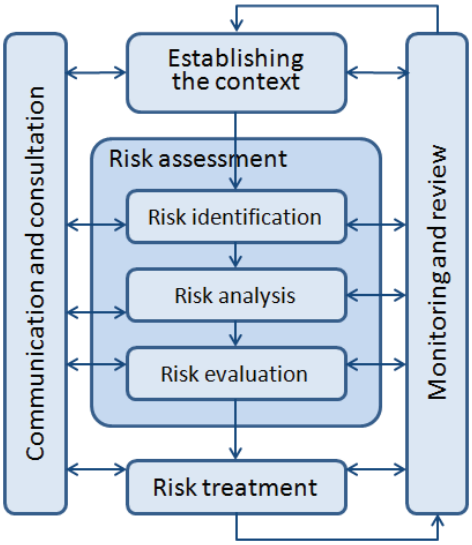

Fig. 2. Risk management process

These common elements (activities) were gathered, shortly described and compared in the PAS99 standard [13].

The analyzed version of PAS99 does not fully address all security standards mentioned in the first chapter of this article, therefore some supplement was necessary and Internal Control Standards requirements were included in this analysis. Table 1 presents a part of this analysis results with the comparison of different security standards and risk management issues.

Similarity of different management systems, like risk analyses elements, audits performance, effectiveness measurement, enables to use (in some extent) the same supporting tool for different standards.

Internal Control Standards	**ISO 27001**	**ISO 27005**	**ISO 31000**	**ISO 22301**
6. Objectives and tasks definition, monitoring and the assessment of their realization	4.2.1 Establish the ISMS	7. Context establishment	4.3 Design of framework for managing risk 5.3 Establishing the context	6. Planning
	4.2.1.c) Define the risk assessment approach	8.1 General description of inf. security risk assessment	5.3.5 Defining Risk Criteria	

7. Risk identification	4.2.1.d) Identify the risks	8.2 Risk analysis	5.4.2 Risk identification	6.1. Actions to address risks and opportunities 8.2. Business impact analysis and risk assessment 8.3. Business continuity Strategy
8. Risk analysis	4.2.1.e) Analyze and evaluate the risks	8.3 Risk evaluation	5.4.3 Risk analysis	
9. Response for the risk	4.2.1.f) Identify and evaluate options for the treatment of risks	9. Information security risk treatment	5.5 Risk treatment	6.2. Business continuity objectives and plans to achieve them 8.4. Establish and implement business continuity procedures
	4.2.1.g) Select control objectives and controls for the treatment of risks		5.5.2 Selection of risk treatment options	
	4.2.1.h), i) Obtain management approval of the proposed residual risks	10. Information security risk acceptance	5.5.3 Preparing and implementing risk treatment plans	
	4.2.1.j) Prepare a Statement of Applicability			

Tab. 1. Risk management process in different management systems

The next chapter presents two examples of such tools. The first is the Pilar tool which supports only risk analysis activities, and the second is a more complex tool – OSCAD [14] which supports also other aspects of the management process, such as tasks and incidents management, audit activities support, etc.

3. Example of risk management supporting tools

Risk management is a subject of different projects and a number of different supporting software tools were implemented up until now. Only few of them were designated or validated in the public administration environment. The examples of such tools, supporting the risk management process according to the EU internal controls requirements and national Spanish regulations, are Pilar and µPilar [15]. These tools are based on the Magerit methodology, which is an open methodology for risk analysis and management, developed by the Spanish Ministry of Public Administration, offered as a framework and guide to public administration [16]. These

tools help to identify existing threats and vulnerabilities, to assess the risk level and to select security measures that reduce risks (Fig. 3).

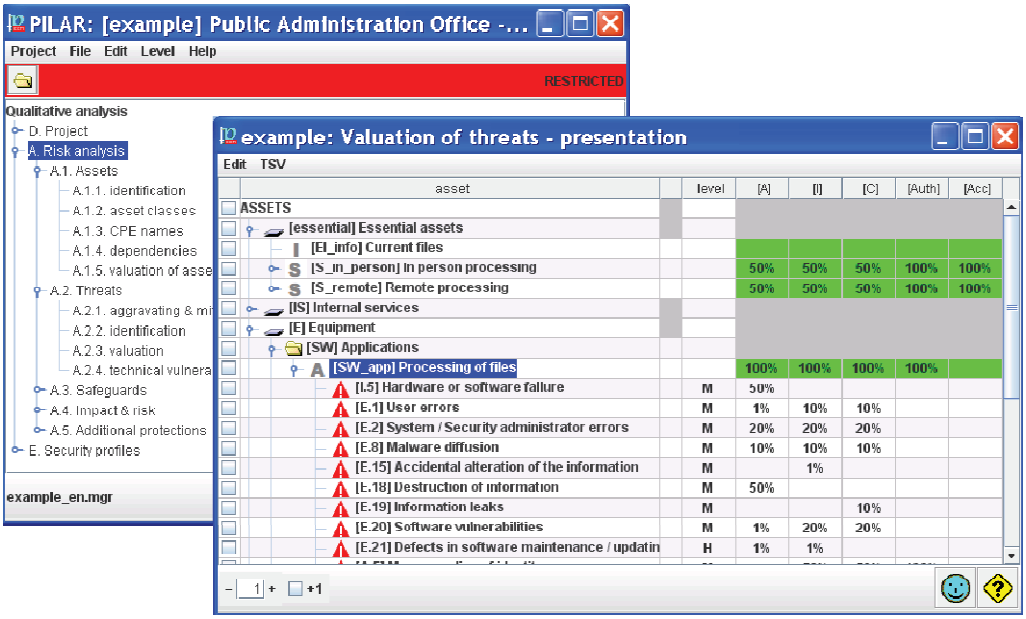

Fig. 3. Pilar – example of risk analysis supporting tool

A similar functionality for the risk management support can be achieved with the use of different software tools, even not directly predestinated for the public administration area. To check this assumption, the OSCAD tool was tested, i.e. its possibility to support management systems in public administration. OSCAD was developed in the EMAG Institute within a project co-financed by the National Centre for Research and Development (NCBiR). Originally this tool was designed as a supporting tool for the information security and business continuity management system. Based on this platform some tests were performed to check how this tool and its risk analysis module can be used to fulfill the requirements of the Internal Control Standards (ICS) and to demonstrate how it supports the risk analysis and the risk management processes.

The results presented in Table 1 were extended with the analysis of extra documents published by Polish governmental units. The list of main requirements of the Internal Control Standards, related to the risk management process, was supplemented with additional detailed recommendations. As a result of this analysis, a mapping table (Tab. 2) was prepared which binds specific requirements and recommendations with OSCAD functions.

Requirements and recommendations	Supported	Supported by OSCAD modul/function
Objectives and tasks definition Monitoring and assessment of their fulfillment	+/- +	Organization configuration Measures and indicators
Risk identification		
Performed periodically	+	Risk analysis and Task management modules
Documented	+	Documents management module
Taking into consideration processes, tasks performed in the institution	+	Business processes description module
Risks identification	+	Risk analysis and configuration modules
Previous incidents consideration	+	Incident management module
Risk owner (custodian) assignment	+/-	Risk analysis module
Risk grouping	+/-	Grouping dictionary
Risk analysis		
Consideration of risk causes	+	Risk analysis module
Assessment of risk significance	+	Risk analysis module (Business Impact Analysis for processes and/or assets, Detailed threats and vulnerabilities assessment)
Two-stage assessment: inherent (current) and residual risk (after controls implementation)	+	Risk analysis module – current/target risk assessment
Additional assessment of controls	+	Risk analysis module – assessment of controls parameters
Definition of acceptable risk level	+	Configuration module
Risk ranking, risk map preparation	+/-	Risk analysis module – analyses statuses
Response for the risk		
Determining the risk treatment activities	+	Risk analysis – selection of new controls; Task management – registration and assignment of tasks for controls implementation
Decision based on the risk level and the costs-benefits of planned activities	+	Risk analysis – comparison of different controls variants (up to 5 variants)

Tab. 2. Risk management requirements in ICS vs. OSCAD functions

In Table 2, the middle column informs if the requirement is fully (‘+’) or partially met (‘+/-’). During the analysis of standards requirements there were no special requirements identified that would be unsupported by OSCAD. Yet, some functions are only partially implemented and could be extended in the future version of the tool. The most important functions which require extension in OSCAD are e.g. risk owner assignment, risk grouping and risk map generation. Taking into consideration other tools supporting the risk management process could be very similar. Thus it seems to confirm the main assumption stated in this article, and it should be possible to use the most of the IT security, business continuity, and other risk management supporting tools in public administration area.

Having in mind these constraints, a case study was performed to prove that the ISMS/BCMS supporting tool (OSCAD) can support the Internal Control process.

The first step of OSCAD tests included configuration, gathering data, information required for this configuration, i.e. typical organizational units, example of processes in public administration, measures used for effectiveness control. These elements were required to check the possibility of internal environment description (organizational structure and employees posts, short information about the organization’s mission and objectives).

The configuration parameters of the OSCAD tool allow to define users’ roles and rights, which is required by chapter 4 of the Internal Standard Controls regulation [3]. During the tests, information about tasks (planned and actual dates of their fulfillment) was used as an element of effectiveness control (control of fulfillment time).

After the configuration, actual activities of the risk management process could be performed. First, criticality of all defined business processes and main information assets was assessed. This activity was supported by the risk analyses module of the OSCAD tool, with the use of the Business Impact Analysis functions. Then, starting from the most critical, important processes and assets, next phases of the risk management process were performed.

Regardless of the risk analyses subjects (processes or assets), the general procedure is almost the same.

Risk identification was performed in compliance with the requirements of ISO 27005 (chapter 8.2), ISO 31000 (chapter 5.4.2) and the standards specified in [6] and [7]. This phase can be supported by the tool through the dictionaries of typical threats, related vulnerabilities (which may cause threats materialization) and security measures (Fig. 4).

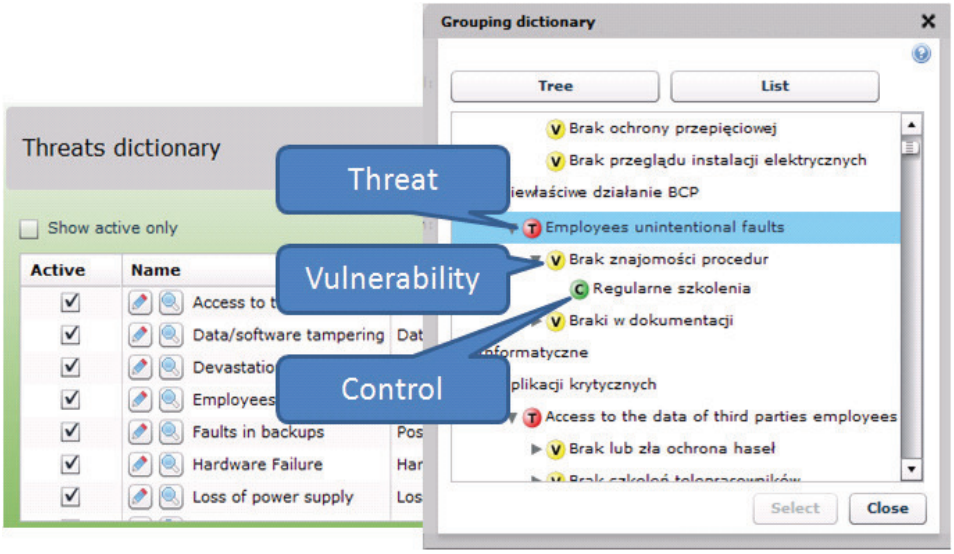

Fig. 4. OSCAD – examples of dictionaries configured for risk assessment

Through defining associations between threats and vulnerabilities (weak points which may cause threats materialization), the OSCAD tool helps to meet the Internal Control Standard requirement of taking into account possible causes of risk.

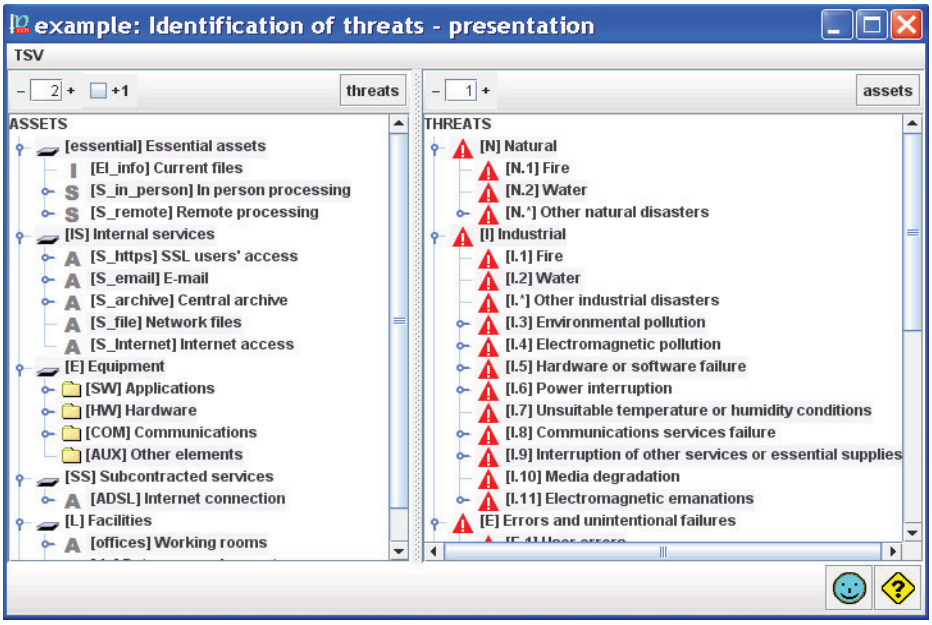

Fig. 5. Pilar – example of threats identification for IT assets

This part of the risk management process is very similar in different supporting software tools. For example, Fig. 5 presents the example of threats identification for IT assets, performed in the different risk management tool – Pilar (already mentioned in this article).

Next, risk level assessment was performed for the selected threats and their vulnerabilities (for processes and assets) which may cause threats materialization, and with respect to existing security measures. The method of risk calculation implemented in OSCAD bases on assessment of possible consequences and probability (or frequency) of occurrence (using the predefined scales configured in dictionaries), extended with two extra controls related parameters. The risk level is calculated with the use of the following formula:

$$R = \frac{I * P}{Ci * Cta}, \tag{1}$$

where R means risk value, I describes impact level, P means probability of occurrence, and values in the denominator are additional parameters used for the controls (security measures) assessment: Ci - controls implementation level and Cta - controls technical advancement level.

Additional assessment of controls allows to fulfill the recommendation of the ministry's guideline ([6], chapter 4.2), which assumes the assessment parameters of existing controls, such as adequacy (influence on possible impacts or cause of risk appearance), efficiency (automatic operation or manual operation of control, dependent on human decision or failure), and effectiveness (cost of implementation does not exceed potential losses).

Afterwards, for the risks which exceed the acceptable, tolerable value, a decision about risk treatment should be taken. In the case of the risk level reduction, when the implementation of new security measures is planned, the next iteration of risk level assessment should be performed. One must assess how the risk level will change after the security measure(s) implementation. Such approach ('two-stage analysis') corresponds with the guidelines presented in ISO standards and is in accordance with the guidelines of the Polish Ministry of Finance ([6], chapter 4.2).

Different security measures variants can be assessed and compared in OSCAD (Fig. 6, Fig. 7). The results of such comparison can be a part of decision support regarding risk treatment activities and controls implementation.

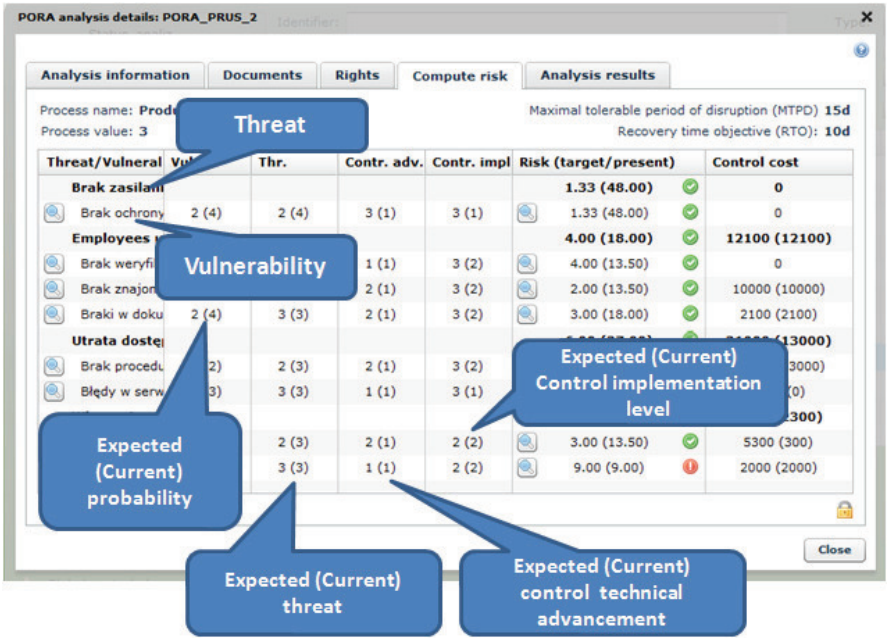

Fig. 6. OSCAD – examples of risk analysis screens

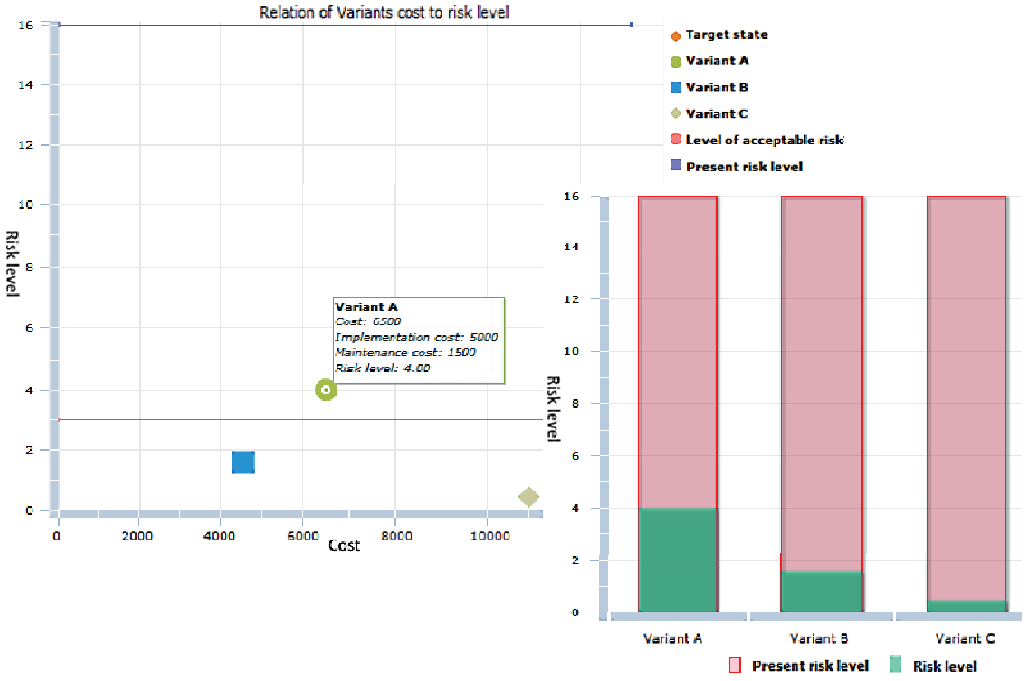

Fig. 7. Examples of security measures variants comparison

Activities performed during the whole risk management process are registered in the OSCAD database. The guidelines presented in [6] include also some templates of paper reports from the risk analyses. The mechanism implemented in OSCAD allows to configure and prepare the templates of electronic documents. Based on them, reports from risk analyses, which are stored in an electronic version, can be also generated as paper documents – PDF files (Fig. 8). It helps the institution management to prove that all required actions are taken.

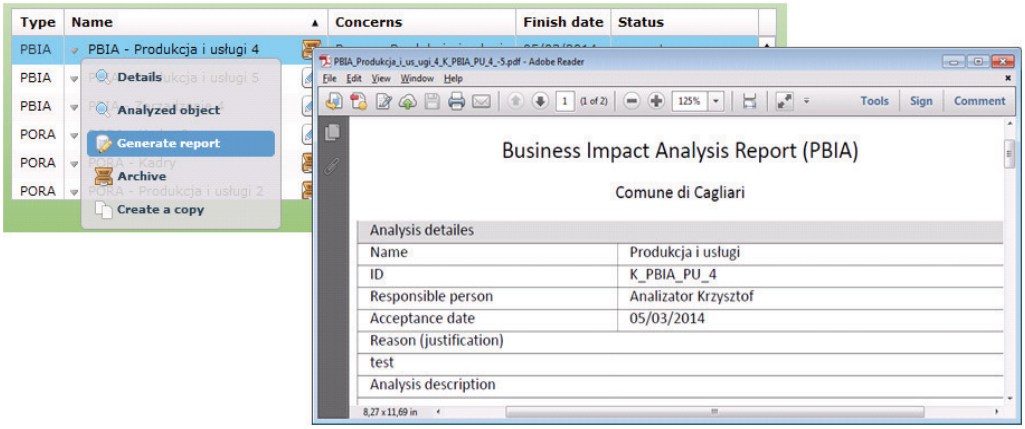

Fig. 8. Generation of PDF report based on the configured template

Apart from the risk management process, OSCAD supports (to some extent) such elements of internal control as: control environment, control activities, information and communication, monitoring.

There are functions available in OSCAD which support such activities as task management with optional users' notification by e-mail or SMS (support of control activities, information and communication), audits (support of monitoring), or defining and logging measures with notification about exceeding acceptable values (support of control activities and monitoring activities) – Fig. 9. The support of these elements can be an added value of using a tool which combines different management systems.

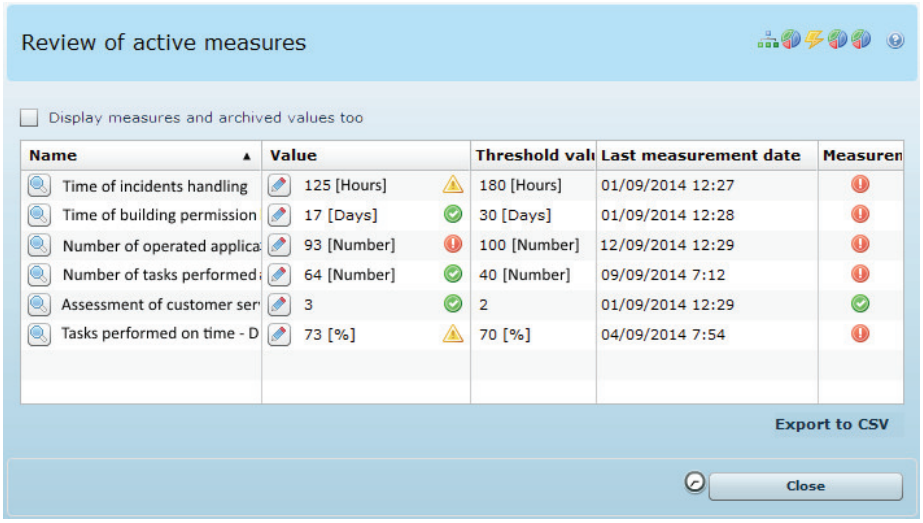

Fig. 9. List of defined measures as a support of control and monitoring activities

The OSCAD tool supports also the incidents management process, including incidents registration, analyses, reports preparation, business continuity plans preparation and execution (by generating notifications about required actions). This functionality was intended to support business continuity systems, but it can be used for registration of disruption regarding any kind of activities performed in the institution. Implementation of business continuity management system

4. Further development possibilities

An issue which is still not sufficiently addressed, neither in OSCAD, nor in Pilar and other risk management tools is wider assessment and comparison of possible impacts of security measures (controls) implementation. Decisions which are taken by public administration may have wide impacts on the society. Therefore they should consider existing conditions in the mentioned different areas, financial and non-financial, and should be based on such information and analyses results. These aspects are not sufficiently addressed in available guidelines. Thus the risk management process should be supplemented with an additional step (in Fig. 10 marked with a dashed line) concerning the assessment of possible impacts of controls implementation. In addition, other positive impacts and possible side-effects will be taken into consideration, such as social, environmental, psychological, political aspects, etc.

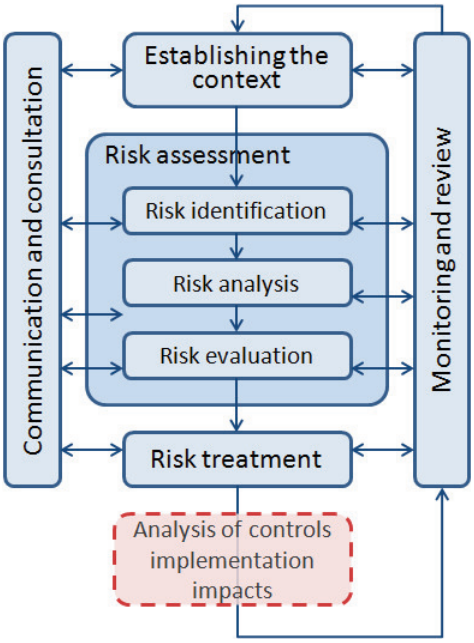

Fig. 10. Risk management process supplemented with additional controls impact analysis

There were attempts to solve this issue during the work on the ValueSec project [17], funded from the 7th Framework Programme. The security management team of the EMAG Institute was also involved in the project [18]. The approach elaborated in ValueSec assumes the support of the decision making process on the basis of results from three pillars: risk reduction assessment, financial costs and benefits analysis, and non-financial criteria assessment (social, political, environmental, and other). However, the software implemented for the support of this solution (Fig. 11) requires external risk analysis tools (during the project validation process those external tools were the tools previously developed by the project consortium members: OSCAD by EMAG, Riger by ATOS, Lancelot by White Cyber Knight, and RAS by the Technical University of Munich). The '3-pillar approach' can be used to support security officers and institution management in decision-making processes in any business area, including public administration.

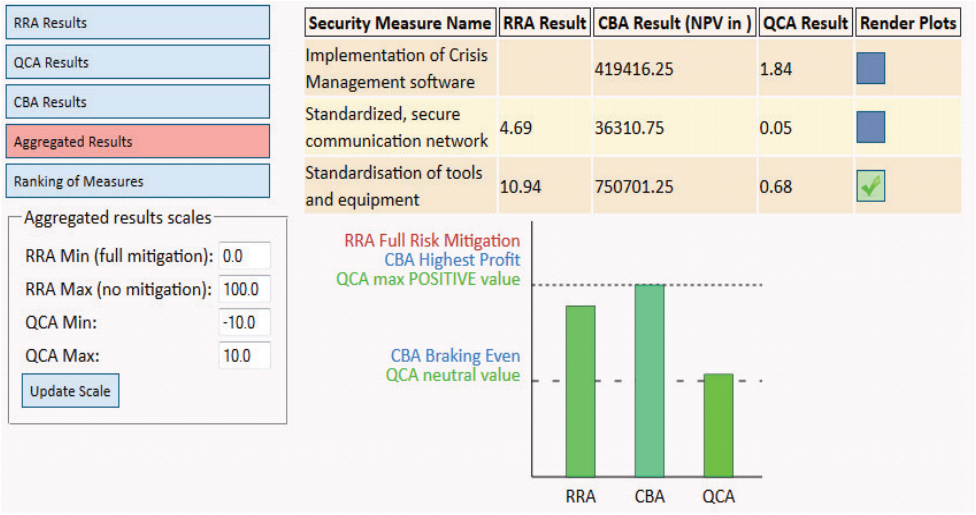

Fig. 11. ValueSec tool – comparison of different security measures assessment results

5. Conclusions

In the article some new legal regulations were presented which affect IT systems managements and information security management in public administration. In chapter 2 main legal acts and current standards were specified. In chapter 3 the author presented some examples of tools which support the implementation of new laws. The OSCAD tool was broadly presented as an example of a tool primarily designated for the Information Security Management Systems in accordance with ISO 27001, but which can support risk analysis activities in different domains. Public administration domain was presented as one of the test cases of the OSCAD tool. Next, some possibilities of further development supporting tools were shortly discussed.

The risk assessment process is the same, in most cases, but different elements of the management process are supported on different levels.

So there is still some work needed and further development possible to extend the risk management process by additional functions, like more advanced decision-making support or the so-called 'soft' criteria, i.e. intangible, non-financial aspects whose assessment should be included in the risk analysis and controls selection process.

The results of risk management should be treated as part of the main input data for the security officers and decision makers (also in the public administration area) during the decision making process of security measures selection. The approach proposed today by the European Commission and national governments (including Polish ministries) can be a good start to apply more advanced methods for the decision making support (e.g. multi-criteria methods, like MCDA – Multi-Criteria Decision

Array) in the future. Software support can help to put in order and unify this process, and to support risk analysis activities of decision makers and security officers in public administration units. The performed tests, related to the risk management software support in the public administration area show that they do not need to start the implementation of Internal Control Standards from scratch. The work shows that software tools for the management systems support, which include risk analyses elements, usually can be adopted to support the requirements of Internal Control Standards. Similar experiments were also performed in other business areas (e.g. coal mining [19]).

Decisions related to the security measures implementation, based on the software support results, can be more transparent and easier to justify if based on clearly defined risk analysis methods and their results.

References

[1] *Law from 29 August 1997 on personal data protection*. Journal of Law 2002, No 101, item 926

[2] *Law from 5 August 2010 on confidential data protection*. Journal of Law 2010, No 182, item 1228

[3] *Communiqué No 23 by the Ministry of Finance from 16 December 2009 on the control standards for the public finance sector*. Journal of the Ministry of Finance No 15, item 84

[4] *Communication to the Commission: Revision of the Internal Control Standards and Underlying Framework - Strengthening Control Effectiveness*. SEC(2007)1341, Brussels, 16 October 2007

[5] *INTOSAI GOV 9100 – Guidelines for Internal Control Standards for the Public Sector*. INTOSAI Internal Control Standards Committee, Approved at XVIIIth Congress of INTOSAI, Budapest 2004, http://www.issai.org/media/13329/intosai_gov_9100_e.pdf

[6] *Communiqué No 6 by the Ministry of Finance from 6 December 2012 on detailed recommendations for the public finance sector about risk planning and management*. Journal of the Ministry of Finance 2012, item 56

[7] *Decree of the Council of Ministers from 12 April 2012 on National Interoperability Framework, minimal requirements for public register and electronic transfer of information, and minimal requirements for IT systems*. Journal of Law 2012, No 0, item 526

[8] ISO/IEC 27001:2005 – *Information technology – Security techniques – Information security management systems – Requirements*

[9] ISO 22301:2012 – *Societal security – Business continuity management systems – Requirements*

[10] ISO 31000:2009 – *Risk management – Principles and guidelines*

[11] ISO/IEC 31010:2009 – *Risk management – Risk assessment techniques*

[12] ISO/IEC 27005:2008 – *Information technology – Security techniques – Information security risk management*

[13] PAS 99:2012 – *Specification of common management system requirements as a framework for integration* (draft version 1.7)

[14] http://oscad.eu or http://oscad.emag.pl

[15] http://www.ar-tools.com/pilar/

[16] http://rm-inv.enisa.europa.eu/methods/m_magerit.html

[17] ValueSec Project, http://www.valuesec.eu

[18] Białas A.: *Risk assessment aspects in mastering the value function of security measures*. In: Zamojski W. et al. (Eds.): New results in dependability and computer systems. AISC, Vol. 224, 2013, Springer-Verlag, pp. 25-39

[19] Białas A.: *Zarządzanie ciągłością działania oraz bezpieczeństwem informacji i innych zasobów w górnictwie*. Mechanizacja i Automatyzacja Górnictwa, Czasopismo Naukowo – Techniczne, Nr 8(510), 2013, Instytut Technik Innowacyjnych EMAG, Katowice, pp. 5—64 (english version: 125-138, russian version: 198-213)

Wsparcie zarządzania bezpieczeństwem informacji i zarządzania ryzykiem w administracji publicznej

Streszczenie

Rozdział dotyczy problemów procesu zarządzania ryzykiem i zarządzania bezpieczeństwem w administracji publicznej i jednostkach sektora finansów publicznych, w odniesieniu do standardów kontroli zarządczej i ich wymagań. W artykule wymieniono i krótko opisano główne akty prawne i standardy związane z tymi tematami. Szczególnie wyróżniono proces analizy ryzyka i doboru zabezpieczeń. Przedstawiono możliwość wykorzystania narzędzi komputerowych do wsparcia procesu zarządzania ryzykiem i doboru zabezpieczeń w jednostkach administracji publicznej. Krótko opisano próbę wykorzystania do tego celu oprogramowania OSCAD. Eksperyment ten wykazał możliwość wykorzystania w obszarze administracji publicznej narzędzia, dedykowanego pierwotnie do wsparcia procesu zarządzania bezpieczeństwem informacji i ciągłością działania. Na koniec przedstawiono możliwości dalszego rozwoju narzędzi wspierających proces zarządzania ryzykiem.