dr inż. Dominika Lisiak-Felicka
University of Łódź

dr Maciej Szmit
Orange Labs Poland

Selected aspects of information security management in Voivodeship Office in Poland

Introduction

Information Security Management System (ISMS) is defined in (ISO/IEC 27000:2012-2.34) as a part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security. The management system consist of guidelines, policies, procedures, processes and associated resources and activities (thus both material resources, such as computers, human resources – as workers, together with their skills and experience, as well as intangible resources – computer programs or organizational culture) to ensure the organization fulfils its tasks and achieves business objectives (ISO/IEC 27000:2012-2.42, Chmielewski J.M. 2006, Humphreys E., 2007, pp. 11-44, Pankova J., et al., 2009, pp. 119-130).

Information Security Management (Ilvonen I., 2011, pp. 148-154, Korzeniowski L., 2005 pp. 20-23, Korzeniowski L.F., 2008) is a great challenge for contemporary organizations and institutions. Offices of government and local government are not an exception in this regard (Korzeniowski L.F., 2012, Kwiatkowski S., 2011, Škvrnda F., 2005, pp. 28-67, Jajodia S., et al. 2010).

Especially, there is a regulation of Polish Council of Ministers regarding to the National Interoperability Framework, the minimum requirements for public registry and information exchange in electronic form and the minimum requirements for ICT systems imposing on managers of public administration units some obligations relating to security management (Rozporządzenie Rady Ministrów z 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych

DOI: 10.5604/18984509.1140876

ISSN: 1898-4509

i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych).

Under paragraph 20, units, which implementing public tasks (one of them is exactly the Voivodeship Office), have to develop and establish, implement, operate, monitor, review, maintain and improve information security management system to ensure the confidentiality, availability and integrity of information including attributes such as authenticity, accountability, non-repudiation and reliability.

There are many reasons why the issues of information security management in offices are interesting, for example:

- Information security in government's and local government's offices has a direct relationship to the cybersecurity and cybersafety (ISO/IEC 27032:2012).
- While each independently decides whether to become a member of one or other system, or to entrust their data commercial company, how to process and store them etc., the processing of citizens data by the authorities is required by law (Ustawa z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie). Possible frauds and computer-related crimes (Meteňko, J., 2005, pp. 24-28) against government information system may affect the security and the safety of all citizens.
- Government offices have a defined scope of its duties and powers, thus it is relatively easy to conduct a comparative study on information security management in various offices. The role "specifics of the company", so important in commercial organizations, is minimal in these offices (Białas A., 2007, (Kister Ł., 2009, pp. 329-334, Robinson N., 2005, pp. 45-49).
- Government offices, due to the principle of transparency and access to public information, are particularly convenient as a research material and – although practice shows that is the tendency to conceal information among employees – responsiveness of inquiries of public administration entities is much higher than for commercial organizations.

1. Aim of the research

The aim of the research (apart from identifying in which government offices are implemented Information Security Management Systems, according to which standards are developed and certified) was finding out the answer to the following questions:

- what are the reasons for which respondents did decide (or not) to implement and certificate ISMS,
- how long it took to implement the ISMS,
- identify problems encountered in the implementation of this system,
- whether they could count on the support of the state administration bodies,
- which factors facilitate the implementation of the ISMS,
- what documentation concerning information security has been prepared in these offices (with the brief overview of it),
- whether the administrator of information security has been appointed, and
- how often IS reviews has been conducted.

The survey is a part of our investigations concerning selected aspects of cybersecurity in government organizations in Poland (Lisiak-Felicka D., Szmit M., 2012, pp. 133-145, Lisiak--Felicka D., Szmit M., 2014, pp 134-144, Lisiak-Felicka D., Szmit M., 2013, pp. 39-53).

2. Method of the research

The research was conducted using a survey questionnaire. For all Voivodeship Offices a letter asking for help in the scientific study by completing a questionnaire was sent. The content of the letter was posted a link to the questionnaire in electronic form, which is located on a server google.com. The annex to the letter with a questionnaire in Microsoft Word file was also sent. In the course of the research many telephone and e-mail contacts with officials was conducted.

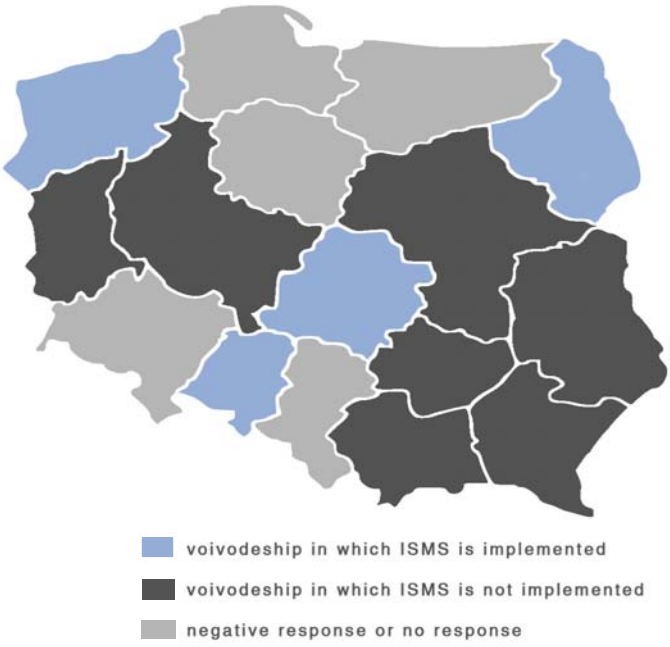
Obtained 11 positive responses. The Kuyavian-Pomeranian Voivodeship Office refused to answer because of detailed technical questions. In the opinion of the officials, answering the questions included in the survey would involve the transfer of sensitive information. Four offices (Lower Silesia Voivodeship, Pomeranian Voivodeship, Warmian-Masurian Voivodeship and Silesia Voivodeship), despite telephone and email communications did not submit any response.

3. Results of the research

Among the 11 Voivodeship Offices, only in four (Łódź Voivodeship Office, West Pomeranian Voidvodeship Office, Opole Voivodeship Office and Podlaskie Voivodeship Office the Information Security Management System is implemented.

The Masovian Voivodeship Office and Subcarpathian Voivodeship Office made attempts to implement the ISMS. In the other five offices such a system does not work and in the past had not been attempts to implement it (see Fig. 1).

Fig. 1. Information Security Management Systems in Voivodeship Offices



Source: Own preparation on the basis of the research.

The declared reasons, why the officials have not taken such action, include: lack of funds, lack of time and lack of sufficient knowledge. The official from the Greater Poland Voivodship Office claims that, at this stage the principles contained in the standards are too demanding. Currently, the office analyzes possibility to decide to implement the system. Lesser Poland Voivodeship Office has not decided to implement the ISMS, because it has the information security policy on protection of personal data and classified information.

All four implemented Information Security Management Systems were developed by the recommendations of the standards, including three offices were using PN-ISO/IEC 17799. One office declared use of PN-ISO/IEC 27001, PN-ISO/IEC 17799 and PN-ISO/IEC 27005. Detailed answers to the survey questions in this area are presented in Table 1.

Tab. 1. Development of Information Security Management Systems

Office	The system developed by the recommendations of the standards
Lódź Voivodeship	PN-ISO/IEC 27001, PN-ISO/IEC 17799, PN-ISO/IEC 27005
Opole Voivodeship	PN-ISO/IEC 17799
Podlaskie Voivodeship	PN-ISO/IEC 17799
West Pomeranian Voivodeship	PN-ISO/IEC 17799

Source: Own preparation on the basis of the research.

All four offices have not decided to certify the Information Security Management System according to PN ISO/IEC 27001, indicated the following reasons:

- it is an expensive proposition (3 answers),
- certification does not affect the quality of the information security management (2 answers),
- it is a time-consuming project (2 answers).

One of the Official underlined that the certification did not result directly from the law until the entry of regulation on the interoperability national framework (Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r.).

Respondents reported the ISMS implementation time. Accordingly, the three offices have identified it as belonging to the range of 6 12 months, one – up to 6 months.

For the success factors and problems with the implementation of the ISMS respondents indicated respectively, as a source of problems: lack of use of formal methods of implementation of the system (4 answers), lack of substantive preparation workers (3 answers), too extensive documentation (3 answers), insufficient financial resources (3 answers), lack of experience of the certification body (1 answer).

Only one office (West Pomeranian Voivodeship) was able to count on the support of the state administration bodies in the stages: monitoring and review of Information Security Management System.

In another question, the officials indicated which of listed factors significantly facilitate the implementation of Information Security Management System. Officials could indicate more than one answer. Evaluation factors with the highest numbers of indications are shown in Figure 2.

Fig. 2. Evaluation of factors that facilitate the implementation of the ISMS

Source: Own preparation on the basis of the research.

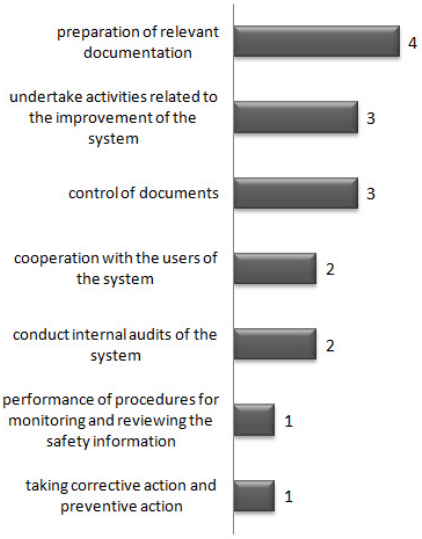
According to officials, the implementation of Information Security Management System has a positive effect on the unit, especially can increase the level the information security, raise the employees awareness of information security management, it is necessary and beneficial. The two officials also indicated that it is an expensive and time-consuming venture. In this questions officials could indicate more than one answer. The numbers of indication of selected answer are shown in Figure 3.

Fig. 3. Opinions on the ISMS implementation

Source: Own preparation on the basis of the research.

Respondents also indicated the steps on the operation of the Information Security Management System, which have the most problems with. In this questions officials could indicate more than one answer. The numbers of indication of selected answer are shown in Figure 4.

Fig. 4. Actions on the operation of the ISMS, which officials have the most problems

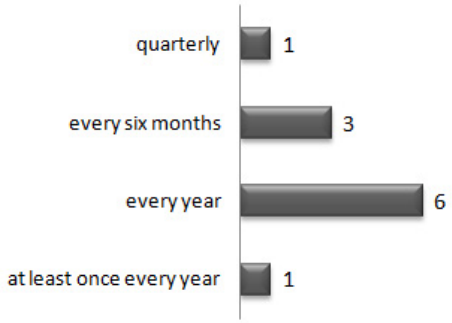


Source: Own preparation on the basis of the research.

Security reviews are conducted in each of the 11 units. The frequency of these inspections is shown in Figure 5.

Among 11 officials, six of them indicated security reviews are conducted every year.

Fig. 5. Frequency of the security reviews



Source: Own preparation on the basis of the research.

Another survey questions were focused on conducting documentation. Among the 11 surveyed offices, 9 have developed and implemented an information security policy that contains the policy of protection of personal data in accordance with the requirements of the Law on the Protection of Personal Data and the two of the offices (Subcarpathian Voivodeship Office and Masovian Voivodeship Office) has only a policy of protection of personal data in accordance with the requirements of the Law on the Protection of Personal Data (Ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych, Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia z 2004, Suchorzewska A., 2010, pp. 279-285).

Table 2 presents the characteristics of each document.

In all of the 11 offices the information security administrators were established and training for employees of the implemented information security policy/protection of personal data policy were conducted.

Officials were asked to indicate the physical security of access to information. In this questions officials could indicate more than one answer.

The numbers of indication of selected answer are shown in Figure 6.

Tab. 2. Characteristics of information security documentation in Voivodeship Offices

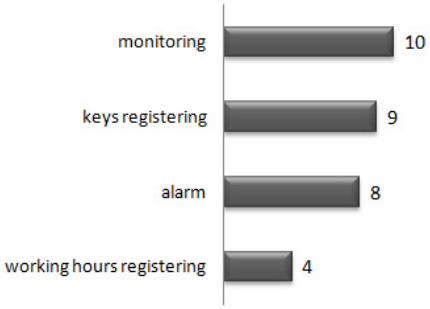
Office	Structure	Approximate number of pages	Last updated	Disclosure of document
Lublin Voivodeship	the main document with attachments	20	2012-10	Only some parts of the document
Lubusz Voivodeship	the main document with attachments	19	2013-06-17	Only some parts of the document
Łódź Voivodeship	the main document with attachments	38	2014	Yes
Lesser Poland Voivodeship	the main document with attachments	163	2012-09-01	Yes
Masovian Voivodeship	one document	10	2013-11-25	Yes
Opole Voivodeship	the main document with attachments	93	2013-07-19	Only some parts of the document
Podlaskie Voivodeship	the main document with attachments	29	2013-12-31	No
Subcarpathian Voivodeship	the separate procedures and instructions	34	2012-09-12	Only some parts of the document
Świętokrzyskie Voivodeship	the main document with attachments	48	2013-10-02	Yes
Greater Poland Voivodeship	the main document with attachments	24	2012-08-13	Yes
West Pomeranian Voivodeship	the main document with attachments	468	2013-12	Only some parts of the document

Source: Own preparation on the basis of the research.

Officials also indicated additional physical security:

- patent locks on the door,
- electronic access control system,
- constant supervision,
- burglar blinds,
- smoke detectors,
- motion detectors.

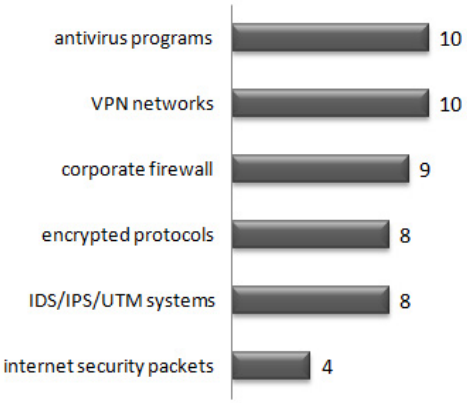
Fig. 6. Physical security



Source: Own preparation on the basis of the research.

Among the implemented security systems (Tipton H.F., Krause M., 2012, pp. 197-666) the most popular are antivirus programs, VPN networks and corporate firewalls. In this questions officials could indicate more than one answer. The numbers of indication of selected answer are shown in Figure 7.

Fig. 7. Implemented security systems

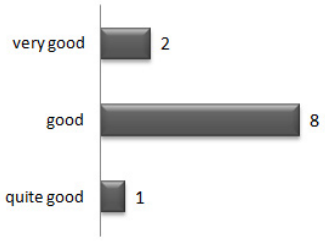


Source: Own preparation on the basis of the research.

The training in information security, information systems security, protection of personal data are conducted in 10 offices (except the Świętokrzyskie Voivodeship Office). Figure 8 shows the evaluation of information security levels in the offices made by the

officials. Among 11 officials, two of them indicated "very good" level, eight of them – "good" and one of them – "quite good".

Fig. 8. Evaluation of information security levels



Source: Own preparation on the basis of the research.

In the five offices (Masovian Voivodeship, Greater Poland Voivodeship, West Pomeranian Voivodeship, Podlaskie Voivodeship, Subcarpatian Voivodeship) also the quality management system are implemented.

Conclusion

On the basis of the results of the research it can be concluded, that the issues related to information security are known for officers, especially in the field of personal data protection. All offices have examined the relevant documentation, in each unit the information security administrator was appointed, all units have adequate physical security of access to information and appropriate security systems. Therefore officials are performing tasks in field of personal data protection.

Based on the responses obtained from the offices in which the Information Security Management Systems is implemented, key success factors have been identified to implement the ISMS. These include: employees awareness of the need to ensure the security of information, involvement of the top management, substantive preparation workers and system requirements in accordance with the specific organization. Therefore, in order to achieve the successful implementation of an Information Security Management System it is necessary to continue raising awareness for employees of all levels of the organization and their respective substantive preparation. This can be achieved through the participation of officials in various training courses in the field of information security. In addition, the subject matter should be addressed in different conferences, involving representatives of the public administration.

Actions on the operation of the ISMS, which officers have the most problems are: prepare relevant documentation, take actions related to the improvement of the system and control documentation of information security. Only one office (West Pomeranian Voivodeship) can count on the support of government units in undertaking activities related to the implementation of the Information Security Management System.

Based on the responses obtained from the offices it can be concluded that officials prepare documentation of information security based on the legal regulations and Polish standards, especially PN-ISO/IEC 17799. Sometimes they use templates.

An important issue is the training of Information Security Management Systems, information security and the personal data protection. The survey results indicate that officials in 10 government offices have the opportunity to participate in such forms of education, although the number of courses in different units are very different (from 1 to about 25). Results of Greater Poland Voivodeship and Subcarpatian Voivodeship seems to be surprisingly good, with a general trend to minimize the government budget, including expenditure on staff training.

On the basis of the research it can be concluded that there is a problem with the understanding which standards include recommendations for the development of Information Security Management System, and according to which standards, the system could be certified.

In summary: the Information Security Management System can be developed based on the recommendations of the standards ISO/IEC 17799 and 27002 (earlier BS 7799-1), and can be certified for the compliance with the requirements of the standards ISO/IEC 27001 (earlier BS 7799-2). See e.g. (Białas A., 2007, Ilvonen I., 2011, pp. 148-154).

In the context of further research, study of Information Security Management Systems in other government and local government units is planned.

References

Białas A. (2007): *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, Wydawnictwo WNT

Chmielewski J.M. (2006): *Polskie Normy dotyczące zarządzania bezpieczeństwem informacji.* Polski Komitet Normalizacyjny, Warszawa, http://193.42.211.16/index.php?pid=GigaCon [2014-04-15]

Humphreys E. (2007): *Implementing the ISO/IEC 27001 Information Security Management System Standard*, Artech House, Norwood

Ilvonen I. (2011): *Information security culture or information safety culture – What do words convey?*, 10th European Conference on Information Warfare and Security 2011, ECIW, Tallinn

ISO/IEC 27000:2014 – Information technology – Security techniques – Information security manafement systems – Overview and vocabulary

ISO/IEC 27032:2012 – Information technology – Security techniques – Guidelines for cybersecurity

Jajodia S., Liu P., Swarup V., Wang C. (ed. Ed.) (2010), *Cyber Situational Awareness*, Springer

Kister Ł. (2009): *Significance of information security in a company*, [in:] *Riešenie krízových situácií v špecifickom prostredí*, Žilinska univerzita, Žilina

Korzeniowski L. (2005): *Securitology – The concept of safety*, "Komunikacie", Vol. 7, Iss. 3

Korzeniowski L.F. (2008): *Securitologia. Nauka o bezpieczeństwie człowieka i organizacji społecznych*. Kraków: EAS

Korzeniowski L.F. (2012): *Podstawy nauk o bezpieczeństwie*, Warszawa: Difin

Kwiatkowski S. (2011): *Zarządzanie bezpieczeństwem w sytuacjach kryzysowych*, Akademia Humanistyczna im. Aleksandra Gieysztora, Pułtusk

Lisiak-Felicka D., Szmit M. (2012): *Tango Down" – Some Comments to the Security of Cyberspace of Republic of Poland*, [in:] *Biały W. Kaźmierczak J. (ed. ed.), Systems supporting production engineering,* PKJS, Gliwice

Lisiak-Felicka D., Szmit M. (2013): *Wybrane aspekty zarządzania bezpieczeństwem informacji w urzędach marszałkowskich*, "Securitologia" 2/2013

Lisiak-Felicka D., Szmit M. (2014): *Information Security Management Systems in Marshal Offices in Poland* [in:] *Information Systems in Management*, Vol. 3, Iss. 2

Meteňko, J. (2005): *Information and communication crime*, "Komunikacie", Vol. 7, Iss. 3

Pankova J., Szankova E., Majernik M. (2009): *Integrated Management Systems In the organization*, "Securitologia" 10/2009

Robinson N. (2005): *IT excellence starts with governance*, "Journal of Investment Compliance", Vol. 6, Iss. 3

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia z 2004 r. *w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych* (Dz.U. nr 100 poz. 1024)

Rozporządzenie Rady Ministrów z 12 kwietnia 2012 r. *w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych* (Dz.U. 2012 nr 0 poz. 526)

Škvrnda F. (2005): *Vybrané sociologické otázky charakteristiky bezpečnosti v súčasnom svete, Čukan K. a kol.: Mládež a armada*, Bratislava: MO SR

Suchorzewska A. (2010): *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Wolters Kluwer Polska

Tipton H.F., Krause M. (2012): I*nformation Security Management Handbook, Fifth Edition*, Auerbach Publications, Florida, USA

Ustawa z 23 stycznia 2009 r. *o wojewodzie i administracji rządowej w województwie* (Dz.U. z 2009 r. Nr 31, poz. 206)

Ustawa z 29 sierpnia 1997 r. *o ochronie danych osobowych* (Dz.U. z 1997, Nr 133, poz. 883, z późn. zm.)

Dominika Lisiak-Felicka
Maciej Szmit

Wybrane aspekty zarządzania bezpieczeństwem informacji w urzędach wojewódzkich

Abstract

The article presents results of a survey concerning Information Security Management Systems (ISMS), which was conducted in Voivodenship Offices in 2014. Survey questionnaires were sent to all Voivodenship Offices in Poland. The aim of the research was identifying in which of the offices ISMS are implemented, according to which standards

ISMS are developed and certified and gathering information about factors facilitate the implementation of the ISMS, problems which occurred during the implementation of these systems and documentation concerning information security. The article is a continuation of research on information security management systems in the state and local government agencies.

Keywords: *information security, information security management systems, ISO/IEC 27001*

E-mail contact to the Authors: dominika.lisiak@gmail.com