Information Security Management in Context of Globalization

Wawak, Slawomir

Cracow University of Economics

January 2012

INFORMATION SECURITY MANAGEMENT IN CONTEXT OF GLOBALIZATION

Slawomir Wawak , Cracow University of Economics

1. Globalization

The idea of globalization became popular in the late 1980s, but the word 'globalization', understood as a process, surfaced in the late 1950s. The problem of globalization has became an issue arousing the most interest among researchers in 1990s .

There are different ways of the globalization concept understanding in the literature. Definitions of globalization can be divided into five categories[1] :

- internationalization, which refers to growing interdependence between countries due to number of transactions, ideas sharing, financial investments, etc.,
- liberalization, referring to efforts to create open, borderless global economy and reduction of regulatory measures and restrictions,
- universalization, which is understood as emergence of homogene worldwide culture, introduction of the same values, legislation, economic and market rules, etc.,
- westernization – variation of universalization, often interpreted as new way of colonization, and thus taken negative,
- relation building, which refers to spread of worldwide connections between people, reduction of barriers in transworld social contacts, as well as changes in global economy resulting from easiness of business cooperation.

The last definition seems to refer to the heart of the problem however internationalization and liberalization should be regarded as significant extension of it. As the practice shows, universalization is an effect of globalization, not a central point. It's impact in different countries is limited by the society's values. Moreover, each society appends its own values to the global culture, which results in its enrichment. It is important to understand, that global and local approaches aren't at odds. Those are two dimensions, which influence and complement each other.

Those changes couldn't be possible without rapid development of technology since XX century. New technologies still play a significant role in globalization. Information technology is the single most important factor to influence globalization.

Sławomir Wawak is an assistant professor of Management at the Cracow University of Economics, Cracow, Poland.

[1] J. A. Scholte, *op. cit.*, pp. 1473-1477.

The globalization also brings threats. Global financial system and global corporations, whose budgets are sometimes greater than GDP of middle-sized countries, are perceived by some authors, as a serious threat to development of countries, as well as a threat to democracy. The last economic crisis seems to confirm those concerns. J. Stiglitz pointed out some negative effects of globalization on developing countries, but also mentioned, that this problem is not related to global trends itself, but to ways of their implementation[2] .

2. Information security management

The security of information should be understood as the provision of confidentiality, accessibility, integrity, authenticity, and accountability of information. Confidentiality is defined by ISO[3] 27001:2005 as “the property that information is not made available or dis-closed to unauthorized individuals, entities, or processes”[4] . Issues about information availability, understood as “being accessible and usable upon demand by an authorized entity[5]” , are not usually seen as a problem of the whole company. Lack of access to data is easily explained away by leave, the lack of electricity, a virus, or missed key. The third main property of information system security is integrity, that is to say, “safeguarding the accuracy and completeness of assets[6]”. It may be considered at a technical level. Then it concerns the structure and configuration of network devices and applications. However, problems of integrity are mainly related to the activities of workers collecting and processing data. Failure to comply with integrity may cause delays in decision-making by management or a lack of actions to minimize the effect of existing threats.

The scope of the information security management system (ISMS) comprises the development of the security policy at the strategic level, the evaluation of the risks relating to threat occurrence, the determination and implementation of security controls aimed at eliminating such threats, and also the monitoring of the systems with the aid of internal audits and a management review. It has been reflected in the structure of ISO 27001:2005 standard that comprises nine chapters. The first four chapters contain an introduction, a description of the scope of the standard, normative references, and also terms and definitions. Key chapters focus on the implementation and maintenance of the information security management system, management responsibility, internal audits, the management review of the ISMS, and information security management system improvement. Such a structure corresponds to other standards established by the ISO that relate to management systems. Doubts may, however, be raised here for the reasons of separating the last three chapters, taking into consideration both the volume and separateness of their contents. In ISO 9001:2000 the review is included as a section in the chapter on management responsibility, while audit is put in the chapter on measurement,

---

[2] Lupan M., Prelipcean G., *Contemporary globalization – confrontations of ideas*, “Annales of University of Oradea” 2009, vol. 2, p. 393.

[3] *ISO – Internation Organization for Standardization*

[4] *ISO/IEC 27001:2005, Information security management systems – Requirements*, ISO, Geneva 2005

[5] ibid

[6] ibid

analysis and improvement, but, it should be mentioned that in both standards these are the same system management tools.

Table 1. Control areas in ISO 27001:2005

Area of control	Groups of controls
Security policy	• information security policy
Organization of information security	• internal organization • external parties
Asset management	• responsibility for assets • information classification
Human resources security	• prior to employment • during employment • termination or change of employment
Physical and environmental security	• secure areas • equipment security
Communications and operations management	• operational procedures and responsibilities • third party service delivery management • system planning and acceptance • protection against malicious and mobile code • back-up • media handling • exchange of information • electronic commerce services • monitoring
Access control	• business requirement for access control • user access management • user responsibilities • network access control • operating system access control • application and information access control • mobile computing and teleworking
Information systems acquisition, development and maintenance	• security requirements of information systems • correct processing in applications • cryptographic controls • security of system files • security in development and support processes • technical vulnerability management
Information security incident management	• reporting information security events and weaknesses • management of information security incidents and improvements
Business continuity management	• information security aspects of business continuity management
Compliance	• compliance with legal requirements • compliance with security policies and standards, and technical compliance • information systems audit considerations

Source: Based on ISO 27001:2005.

The key part of ISO 27001:2005 is Annex A that contains a list of security controls divided into the following groups: security policy, information security organization, asset management, personnel security, physical and environmental security, system and network management, system access control, information system development and maintenance, information security incident management, operational continuity management and compliance assurance. The security groups are strictly related to the contents of the ISO 17799:2005 standard where detailed guidelines concerning the implementation and monitoring of security controls may be found. It should be noted that in many cases the ISO 17799:2005 standard deals with an information technology system however, in the case of implementing the information security management system, it should be interpreted more broadly, as an information system. A full list of areas and the controls is shown in table 1.

While developing standards for management systems, the International Organization for Standardization complies with the principles of their compatibility and complementarity. Apart from ISO 27001, the most popular standards in this field also include systems of quality management, environment and occupational safety. The compatibility is seen in the application of similar management methods and tools, e.g. principles of supervision over documents and records, the development of organizational policies, carrying out management system reviews, internal audits, identification of non-conformities (or incidents), corrective and preventive action. Such an approach facilitates the simultaneous implementation of systems. It is also worth noticing that in the case of the disunited implementation of standards, the solution that works best is the one in which the organization implements the quality management system first, encompassing the entire company, acquainting the employees with new working methods. Management systems developed by ISO complement each other well, allowing for the development of an organization towards the total quality management (TQM) concept.

Information security management systems are applied in a number of sectors of the economy. They are used by production and service companies, businesses that provide information technology and telecom services, state administration authorities and local governments. Those systems are implemented to protect from external actions, illegal actions of staff, as well as to prepare in case of crisis situations.

Protection against external actions is related to introduction of limitations of physical and electronic access by persons from outside an organization, and also to implementation of tools recording contacts between the external environment and the company's information technology system. This may include instituting industrial security service, access cards, encryption protocols for data transmission, additional security controls for logging with the use of keys of tokens, etc.

Protection against internal actions refers to persons who stay in the organization's premises, or primarily all employees. Following implementation of such controls, access to selected premises is limited, physical security controls securing stored information and limits on electronic contact within the company are introduced. Implementation of actions focused on employees may have a strong impact on their motivation level for work, therefore it shall be necessary to include changes in the incentive system, and also employee training shall have to be carried, making them aware of reasons for imposing such restrictions.

The third direction of ISMS implementation concerns preparation of plans in case of an insufficient level of security controls. Such a situation may occur as a result of underrating importance of threats, their willful acceptance further to a low probability of their occurrence or impossibility of implementing costly security controls. Prepared plans may concern responses to threats, the sequence in which people, documents, and equipment are saved, quick recovery of the organization's part following a breakdown.

The key ISMS tools are:

- management review,
- corrective actions,
- preventive actions,
- incident management,
- risk assessment,
- risk treatment plans,
- compliance metrics,
- internal audit.

Management review. Management review is a regular meeting of executives dedicated to the functioning of the system. The main reviews are held several times a year, but short meetings even several times a month. Reviews allow to gather information, enable information comparisons and entail discussion between representatives of the organizational units. In this way the review causes that each participant better understands the situation of the company. Management review promotes the understanding of relations between different parts of the organization. Understanding those relations enables managers to more accurate detection of the problems.

Corrective actions. The aim of corrective actions is removal of non-compliance and incidents causes. These actions are taken based on information about identified noncompliance. Information security manager is responsible for the proper conduct of actions, While the employees according to their competencies are responsible for causes removal. Quick removal of causes makes possible to minimize adverse effects, as well as immune company of a given type of causes.

Preventive actions. Preventive actions serve to detect and remove potential causes that could entail non-compliance or incidents. Their carrying requires involvement of all employees in order to identify potential problems. Procedures of running these actions are the same as in the case of corrective actions. Identification of the causes allows finding further causes of problems and better understanding the organization and its environment. Moreover, removal of causes will imply that there won't be any adverse effects. Preventive actions are more difficult to implement, but they are more efficient (no losses).

Incident management. Detection of undesired events and quick response to it is the goal of incident management. In addition, it provides information for corrective action. Identification and reporting of incidents is the responsibility of every employee. This tool increases the workers' awareness and sensitivity to the problems occurring in the company and its environment.

Risk assessment. Risk assessment is the periodic review of risk factors and identification of new factors. General assessment is usually done once a year. Besides it, during the year are carried out a number of minor assessments. Conducting risk assessment immediately after the identification of changes in risk factors provides the information necessary to take preventive action and update risk treatment plans.

Risk treatment plans. Risk treatment plan is a set of instructions followed in the event of a risk factor. The organization should make plans on the basis of risk assessment, audit reports and information from the outside. Valuable source of plans are simulations. Current and possible to implement plans should be practised, because when a problem occurs, there is usually no time to learn instructions. The employee who is able to recognize triggers, can automatically take action to reduce the impact of the causes that could entail a crisis in the company.

Compliance metrics. Compliance metrics are a set of metrics to monitor the functioning of the system. Not only the computer system, but the whole organization should be monitored. It is possible to create a measurement system based on the assumption BSC, which will set up an early warning system. Using precise metrics allows earlier detection of irregularities. However, the high accuracy of measurement increases costs of measurement. It should be noted that the use of individual metrics has little influence on the security of the organization. It is necessary to use a coherent system to achieve this effect.

Internal audit. Internal audit is a tool for monitoring specific areas of business and processes. Its main objective is to improve the information system. This is achieved through cooperation between the auditor and auditee. A secondary purpose is non-compliance detection. Audit perfectly complements the other methods because it uses a less formal, flexible approach. This makes it possible to detect risks that are not identified by other tools.

3. Information security in global economy

Development of the information technology accelerates growth of globalization, however, this relationship is two-directional. Global economy affects the ways of thinking about information management. Awareness of this fact among the company executives grows, but still is insufficient. The major roles in top management decisions are played by economic effects, whereas information security problems are often overlooked.

The cost effectiveness is an important factor for shareholders, thus outsourcing of expensive information technology departments is welcome. For example, a system integration job in India or Russia might cost one-fifth of the amount which had to be paid in USA.

Correct calculation of the cost should, however, take into account the risk of security problems. The awareness and appreciation for information security of personnel can be significantly less in some countries. Moreover, there should be considered other threats, e.g.: political risk, industrial espionage, intellectual property theft, as well as disaster recovery issues.

The cost cutting results also in reduction of audits number in overseas departments. Lack of control can lead to loosening of security procedures, and increase of security incidents[7] .

It should be noted, that information security is nowadays still in infancy. Methods, techniques and procedures, which are used, aren't up to speed with trends in the global economy. Information security issues are taken into account on the last steps of software production, and thus they are an overlay, not one of central functions of applications. This causes many security holes.

Companies, whose implemented information security management systems, frequently build security bureaus detached from other departments. This produces duality where the aim of core departments is production or services, and security issues are concern of IS bureaus. It results in information security confusion with only computer systems security.

Although there are several standards for information security management systems, there are no well-established rules of ISMS yet. Moreover, those systems don't include such important issues like knowledge security or how to effectively protect knowledge of the staff released. It is doubtful if such principles can be developed, while information technology still grows fast[8] .

In conclusion, the challenge for the coming years is treating information security as an important business enabler, not only an additional feature.

4. Approach to information security in Poland

Approach to information security in Poland has changed considerably in recent years. An increasing number of malware and viruses has led the companies to start using basic security technology. Attacks on information systems, aired on the media, entailed that the top management of companies became increasingly aware of the risks.

In recent years, a series of legal acts related to information security were published, including: protection of personal data (1997), protection of classified information (1999), providing electronic services (2002), computerization of public service (2005), ICT [9] requirements (2005), minimum requirements for information systems (2005) and others.

In the following part of the paper, there will be presented results of the research concerning the level of information security management in local government administration in

[7] W. Madsen, *Globalization of services: GATT, NAFTA, and the threat to information security*, "Information Systems Security" 1995, vol. 4, iss. 2.

[8] Choobineh J., Dhillon G., Grimaila M. R., Rees J., *Management of information security – challenges and research directions*, "Communications of the Association for Information Systems" 2007, vol. 20.

[9] ICT information and communication technology

Poland, conducted by the author in 2011[10]. The study involved 179 local government offices, which represents approximately 5% of the offices of this type in Poland.

Only 67% of the offices provide services electronically. The number of services varies from one to a dozen. In half of the offices complaints are accepted, requests and inquiries to the office headed by the national system for electronic communication with public administration (e-PUAP)[11] or their own solutions (electronic inbox). A large number of respondent are allowed to deal with matters relating to the register of voters and business records. Other services are carried out electronically in the individual offices, these include: providing public information, providing active forms and applications, provision of tax information, licensing for felling trees or the sale of alcohol, the case of civil registration, identity cards and census, and also monitoring the status of the case (Fig. 1).

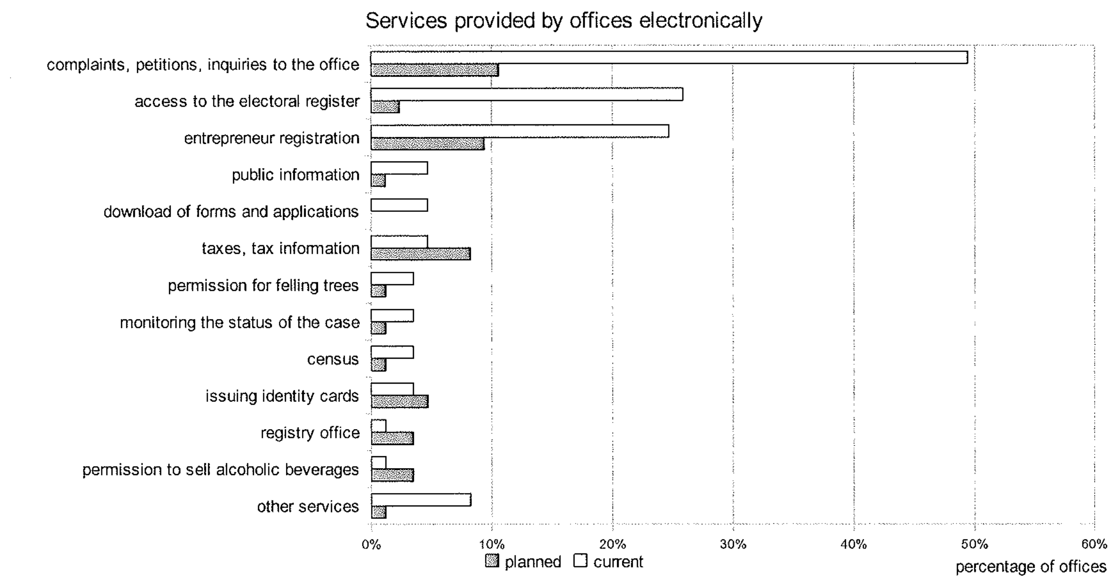

Fig 1. Services provided by offices electronically

The weight given by the management office for information security is low. As many as 54% of offices did not organize in 2010 any meetings on the IS, and only 12% of offices held them every three months. Most offices have limited information security management to meeting the requirements of the law (protection of personal data, some security technology).

Offices have little training in information security (Fig.2). It is associated with a reduction in the number of training days. In 2004, there were more than 10 days of training per employee, and in 2010 only 2.43 days.

[10] Full research reports have been published online at http://www.wawak.pl.

[11] e-PUAP: electronic plat form of public administration services

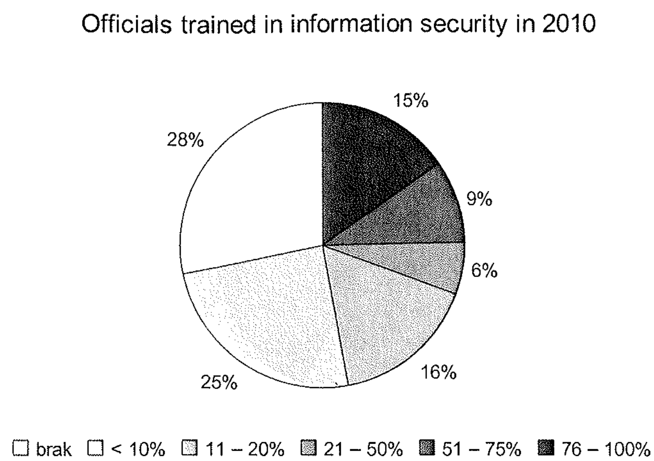

Fig 2. Officials trained in information security in 2010

The availability of procedures and instructions for employees has a significant impact in reducing the frequency of errors. In civil service, officials directly use the legal acts which are not always convenient and easy to interpret, but it gives up to date instructions. However, with regard to information systems and information security, the number of such documents is small and not sufficient to achieve a high level of quality of work.

Just a little over half of office workers have access to the documents describing the operation of computer systems. This is a very low score. Situation is even worse in the case of IT specialist instructions. Usually it is assumed that as a professional operator, does not need detailed instructions. However, when a new employee is hired on this post, if there is no manual for making backup, starting and stopping systems, etc., he will lose a lot of time learning the specific system configuration, and can cause a lot of incidents or breaches.

It should be noted that due to low salaries in local government compared with private firms, fluctuation of staff in IT positions is high. Often work in the office is seen as a first step in a career or a cheap way to undergo expensive training to raise skills.

In 57% of office audits of information security have not been conducted in 2010 (Fig. 3). In 39% of the office audits have been conducted internally. Only 4% of offices have decided on external audits. Research carried out by workers are cheaper and can be conducted more frequently, which is their advantage. A disadvantage is the possibility of lenient treatment of certain practices in the office (unwarranted show of understanding for security breaches to facilitate the work), and fall into a rut, as well as ignoring new threats (no development). The optimal solution is therefore a complement of internal audits with external audits.

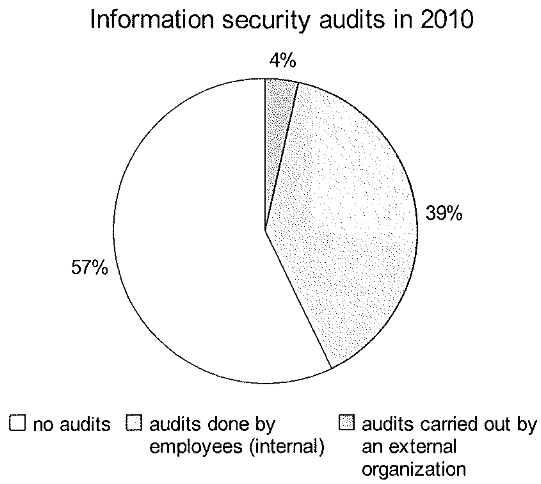

Fig 3. Information security audits in 2010

The next two questions concerned the availability of different types of information to employees and customers. Respondents were asked to assess the availability in the 1-4 scale, where:

- 1 – no access,
- 2 – limited access,
- 3 – sufficient access,
- 4 – fast and reliable access.

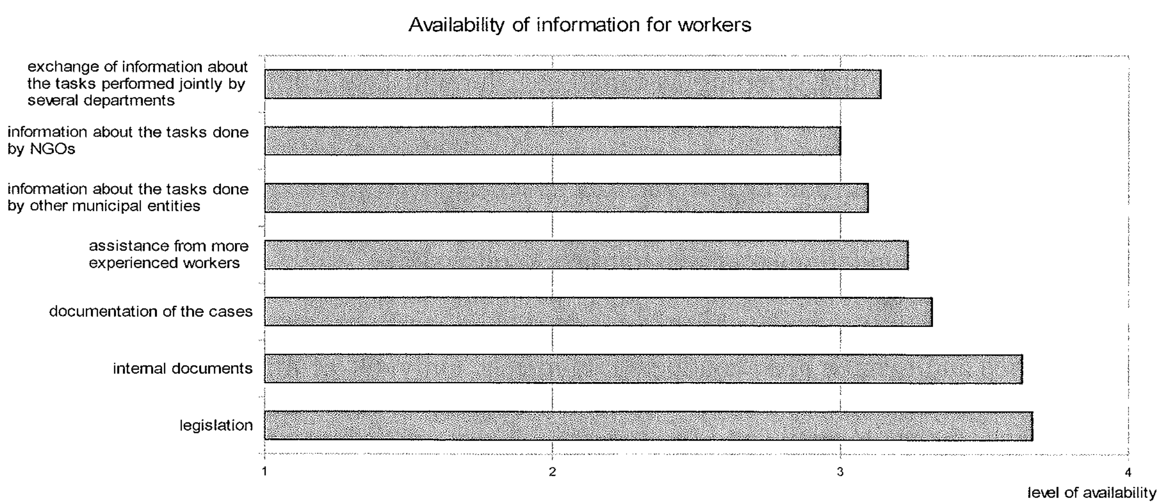

Fig 4. Availability of information for workers

The results of analysis were shown in Figure 4 and 5. The answers given by the respondents were very similar, as evidenced by low standard deviation of the response (below 0.5). Respondents estimate that access to information for workers is good. Only the information about tasks by NGOs are below a sufficient level. Both access to documents and legal acts, as well as exchange of information between employees and departments were rated good.

A little worse, officials assessed the availability of information to citizens. It was recognized that access to legislation and workers assistance were least sufficient. In contrast, the availability of the documentation of cases and information about the stage of cases realization is perceived much worse. Online access to information about stage of cases realization was assessed as the worst. These are the areas where improvement is highly desired.

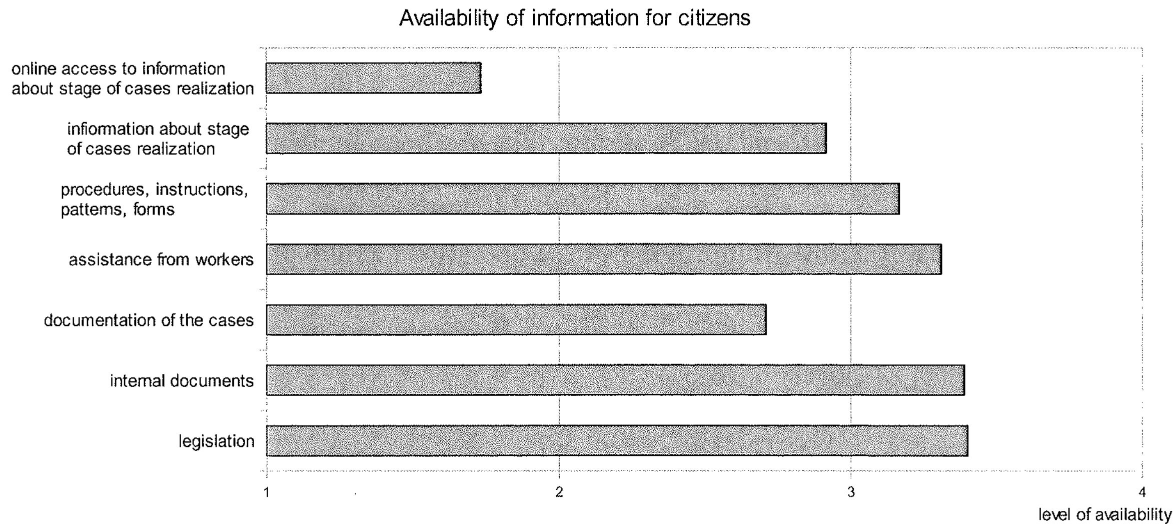

Fig. 5. Availability of information for citizens

The communication between the office and the residents is an important factor associated with information management. It influences the assessment of the quality of its work by the citizens. Awareness of inadequate access to information should be a signal for the reorganization of information policy in this area and for an increase of the information availability.

5. Conclusions

Globalization is a process that requires organizations to adapt the methods of business. One of the directions of adaptation is the improvement of the information security level. This can be done through the implementation of ISO standards.

The implementation of the information security management system is a process that is by far more complex than the implementation of the quality management system due to the large number of factors that may affect its effectiveness. It thus becomes necessary to ensure highly qualified staff, who have skills, not only in the field of information technology, but also know the principles of how to implement management systems on the basis of ISO standards well. An increased awareness of the organization's management is also necessary.

An effective information system should: provide employees with access to necessary updated and reliable information that is required for their job positions, eliminate information that is redundant for the job position to prevent information overload, limit access to confidential information, including the prevention of drawing conclusions on the basis of a large number of non-classified information, have a high capability of recovery following the occurrence of adverse events or human actions, ensure the company's communications with the environment on the basis of assumptions concerning confidentiality, availability, and the integrity of information.

The above presented selected results of research show the state of information security management in local government administration in Poland. It should be noted that a large number of offices do not pay enough attention to the problems of information security.

The ISO 27001 standard takes into account the most important aspects of information security that the office should focus on. A system that has been implemented on its basis may easily be integrated with other systems that are based on ISO standards. The introduction of the information security management may be treated as a stepping point towards the reorganization of information systems in terms of improving office operations and expediting the development of the local government.

Bibliography

Archibugi D., Iammarino S., The globalization of technological innovation: definition and evidence, "Review of International Political Economy" 2002, March

Choobineh J., Dhillon G., Grimaila M. R., Rees J., Management of information security – challenges and research directions, "Communications of the Association for Information Systems" 2007, vol. 20

ISO/IEC 27001:2005, Information security management systems – Requirements, ISO, Geneva 2005

Lupan M., Prelipcean G., Contemporary globalization – confrontations of ideas, "Annales of University of Oradea" 2009, vol. 2

Madsen W., Globalization of services: GATT, NAFTA, and the threat to information security, "Information Systems Security" 1995, vol. 4, iss. 2

Scholte J. A., Defining Globalisation, "The World Economy" 2008, vol. 31, no. 11