Information Security Issues within Local Government

Wawak, Slawomir

Cracow University of Economics

2009

Information Security Issues within Local Government

By Sławomir Wawak

Abstract: *Local government offices in Poland are required to apply information security controls that are provided for under Polish regulations of law. The standard of ISO 27001 treats the security issue much more broadly, extending it to the entire information technology system. Due to that reason offices that are considering the need of improving their information technology systems more frequently use information security management systems. The paper discusses selected issues relating to the implementation of such systems.*

Introductory remarks

The security of information should be understood as the provision of confidentiality, accessibility, integrity, authenticity, and accountability of information (A. Białas 2007, p. 34). Within a modern organisation it is often misunderstood to be the field of computer specialists who install hardware and software. Companies and offices invest in firewalls, anti-virus software, data encryption systems, etc. Thus, the top management is convinced about the high level of security.

The basic criteria of assessing technical security controls relate to their costs and the time needed to break them. It is impossible to develop a system that will be fully secure (R. Anderson 2005). The majority of technical security controls may be bypassed, if there are no organisational security controls in place. Companies and offices are not able to cope with the implementation of such controls. Research has shown that over 50% of employees who have been fired or leave, copies and takes away classified data.

The purpose of the paper is to discuss selected issues concerning information security in local borough council offices in Poland and show ways of solving them with the use of an information security management system. The requirements of the information security management system proposed under the standard of ISO 27001:2005 have been adopted as the basis for the discussion offered in this paper. Though it does not constitute a complete source of knowledge about the field, it does, however, provide a very comprehensible structure of the issues relating to information security, and also indicates the necessity of applying a process approach. Considering the implementation of security controls without a

complex analysis and process review is doomed to fail, as numerous authors have pointed out.

Assignments of local borough council offices in Poland

Assignments of local borough council offices in Poland are governed by the Act on Self-Government in Communes. Among others they include matters such as (*Act on Self-Government in Communes*, Art. 7.1):

- spatial order, real property management, protection of the environment and nature, and water management,
- arrangement of the road traffic,
- local public transport,
- health care,
- social security,
- public education,
- culture, including libraries, centres of culture,
- physical leisure and tourism,
- local trade,
- public order and the safety of citizens,
- promotion of the local borough,
- co-operation with non-governmental organisations,
- co-operation with the local and regional communities of other states.

Offices carry out some of the assignments by using auxiliary organisations: municipal guards, public utility companies, and unit managing schools, health care centres.

A review of the list of assignments shows that information security issues are very broad and differentiated. Major problems relating to information security management in local borough council offices include:

- limiting access to the personal data of citizens and employees,
- ensuring proper access to public information,
- ensuring the transparency of operating procedures applied in the office,
- ensuring permanent access to information about the office,
- the integrity of information provided to clients,
- the update of information used for decision-making,
- accountability of civil servants for their performance at work.

Access to personal data is governed by the Personal Data Protection Act. Offices are required to observe the confidentiality of personal data and appoint persons who have access to them. Data collected in the citizens' registers that issue identification cards and in the registry of vital records and statistics should be subjected to specific protection. There, it is is necessary to develop procedures making information available to citizens, and also institutions like: courts, the police, and other authorities. Presently, it is relatively easy to steal personal data using the trust civil servants have to other public institutions.

Offices should provide citizens, investors, and the mass media with access to information about public matters, pursuant to the Act on Access to Public Information. Such information concerns the development plans of boroughs, drafts of legal acts, financials, etc. In certain cases, civil servants try to limit the access to such information, since making some of it public may result in protests staged by citizens or adverse feedback from investors. Governing access to such information may also be the source of illegal benefits for civil servants. The issue is closely related to the provision of transparency of how offices operate.

Local borough council offices that have implemented the quality management system ISO 9001, and also CAF, care more and more about providing access to updated information about the procedures applicable while handling official matters. It expedites customer services, and also limits the necessity of visiting the office many times. Unfortunately, less than 10% of offices in Poland have certified quality management systems in place. Non-updated or incomplete information significantly impedes the provision of services and adversely affects the assessment of the quality of the office work by citizens.

The issue of having updated information is also critical for internal processes, where employees must have permanent access to updated legal acts, reports, and analyses to be able to take appropriate decisions. It requires the improvement of the flow of information.

The accountability of civil servants is the last of the issues that has been mentioned. It is assumed that administrative decisions are issued by the office. They are signed by the head of the office. In the event whereby errors have been found in a decision it is the office that is held responsible, not the civil servant who has committed the error. Removing the liability from civil servants makes some of them unwilling to improve their work and thus they commit the same errors many times.

Information security management system

The scope of the information security management system (ISMS) comprises of 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 system with the aid of internal audits and a management review. It has been reflected in the structure of ISO 27001:2005 standard that comprises of 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, analysis and improvement, but, it should be mentioned that in both standards these are the same system management tools.

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 organisation, 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.

The ISO 13335 standard that currently comprises of two sheets forms a background for implementing the ISMS as it provides general knowledge about the models and concepts of the information system management. It presents a number of security aspects at various levels of the organisation: corporate, interdepartmental, departmental, or in the IT area. It contains guidelines both concerning the methodology of risk evaluation, and detailed principles of securing information technology systems.

While developing standards for management systems, the International Organisation for Standardisation 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 organisational 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 organisation 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 organisation towards the total quality management (TQM) concept.

Implementation of the ISMS in local borough council offices

The procedure of preparing and implementing the information security management system has been described in clauses 4.2 and 4.3 of the standard [*ISO 27001:2005*, s.9]. It is made up of the following steps:

- defining the scope and boundaries of the ISMS,
- defining the ISMS policy,
- defining the approach to risk assessment,
- defining the risks,
- analysis and evaluation of the risks,
- identification and evaluation of risk treatment options,
- selection of controls,
- approval of all residual risks,
- obtaining authorisation for system implementation,
- preparation of a statement of applicability,
- development of a risk treatment plan,
- implementation of the risk treatment plan,
- implementation of security controls,
- defining the ways of measuring effectiveness of security controls,
- training of employees and associates.

The scope of the information security management system may not be freely defined, since it has to take into account the nature of operations pursued by an organisation. It is a mistake to subjectively or objectively limit the system that may cause its incomplete

efficiency. The office management usually imagine, at the outstart, that the information security system will operate in the server room and the classified information bureau. Such a solution, however, would not include the number of job positions that are responsible for observing the confidentiality or maintaining the continuous access to the information. The system should thus encompass the entire local borough council office, together with subsidiary organisations that perform local council works.

A good solution is to integrate the ISMS with the quality management system. There are a number of similarities between the two systems, such as the structure of documentation, at the top of which there is the ISMS policy. Its task is to define the major directions and principles of operations with regard to the provision of information security. From the point of view of strategic management, the policy may be treated as an element of strategy concerning the proper functioning of the information system. Such an approach, in the case of an integrated management system, allows for the easier management of many policies pursued in the office.

The development of the risk evaluation method is a key stage of designing the information security management systems. The ISO 27001:2005 standard does not point to any specific method, leaving some freedom in this respect. Such an approach is justified, since systems are implemented within different organisations. A proposal of the method is, however, included in the ISO TR 13335-3:1998 standard. Although it is limited to information technology systems, it may easily be adopted to a broader category such as an information system. The method must be prepared in such a way that it will provide for its multiple repetition and ensure the comparability of results. It should take into account not only legal requirements, but also those relating to the operations pursued by an organisation. The method must contain criteria that will allow for the definition of acceptable levels of risks, and on that basis, taking a decision about acceptance.

The ISO 27001:2005 standard requires risks to be defined in four steps:

1) identification what assets (information, hardware, etc.) are in the organisation in terms of ISMS implementation and who is responsible for them,
2) identification as to what could pose a threat to such assets,
3) identification of susceptibilities, or weaknesses of such assets that may be used by threats,
4) identification of the consequences for the assets that may occur in the event of threat occurrence.

The standard does not clearly indicate that threats and susceptibilities should be identified individually for each type of assets; however, auditors who certify systems are

unenthusiatic about methods in which susceptibilities have been defined in groups. Risk identification is a time consuming activity and requires the participation of representatives from all the organisational units. Due to this, its optimum form includes training sessions combined with workshops.

Risk analysis is performed on the basis of the identification results. Its purpose is to show the losses that a default on confidentiality, accessibility, accuracy, or the integrity of assets may cause. Next, the likelihood of the occurrence of incidents that default on security and losses should be indicated, taking into account the currently applied security controls. Based on that, it is possible to estimate the risk level and take decisions on whether it is acceptable, or whether it is necessary to undertake additional preventive actions.

The standard proposes four solutions: the introduction of security controls, knowing the acceptance of risks, risk avoidance or their transfer to other organisations, e.g. insurers. The choice of security controls is facilitated by a list of over 100 proposals that has been presented in the standard implementation, which should be considered. The list has been prepared on the basis of information security management principles published in the ISO 17799:2005 standard.

Acceptance of residual (acceptable) risk by the management and an implementation approval constitute a passage from the design stage to the implementation stage of the information security management system. A statement of applicability of the ISMS, which is the outcome of the completed design stage, contains a description of the selected and implemented security controls, and also of any possible reasons for excluding certain security controls recommended by the standard.

Research conducted by the author in several local government offices has shown that technical security controls are used at a good level. Unfortunately, organisational security controls are at a satisfactory level. This is so because the implementation of technical security controls is the responsibility of an information technology officer, who has the relevant qualifications, whereas the organisational security controls are the responsibility of all employees. The implementation of such security controls will require substantial changes in the organisation's culture.

Due to that reason the implementation phase should be accompanied by a series of employee training courses. Their purpose is to acquaint employees with the new ways of the work organisation and to explain the reasons for introducing changes. Next, there comes the development and implementation of the risk treatment plan that will define the actions that need to be undertaken, their sequence, and the positions that are responsible for the

introduction of changes should be indicated. The further stage includes the implementation of security controls provided for in the statement of acceptability, and defining the way of measuring their effectiveness. The measurement should allow not only for the assessment of system operations in the future, but also the results of comparisons of changes in time.

Summary

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 organisation's management is also necessary. The lack of management decision about the technology to use, seeking to apply fashionable information technology tools or apparent savings in the introduction of innovations may make the office more susceptible to threats.

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 reorganisation of information systems in terms of improving office operations and expediting the development of the local borough.

Bibliography

Anderson R., *Security engineering: a guide to building dependable distributed systems*, John Wiley & Sons, 2001

Białas A., *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, WNT, Warszawa 2008

ISO 27001:2005 Information technology – Security techniques – Information security management systems – Requirements, ISO, 2005

ISO 17799:2005 Information technology – Security techniques – Code of practice for information security management, ISO, 2005

ISO TR 13335-3 Information Technology - Guidelines for the management of IT Security - Part 3: Techniques for the management of IT Security, ISO, 1998

Kelly E., *Laid off workers likely to steal company data, survey warns*, http://

searchsecurity.techtarget.com/ news/article/0,289142,sid14_gci1348948,00.html, 2009

Ustawa z dn. 8.03.1990 o samorządzie gminnym, Dz. U. 2001.142.1591

Address:

Dr Sławomir Wawak

Chair of Process Management, Krakow University of Economics

ul. Rakowicka 27, 31-510 Kraków, Poland

wawaks@uek.krakow.pl

www.wawak.pl