Chapter VII

INFORMATION SECURITY MANAGEMENT

1. Information Security Management [ISO/ IEC 27001]

The word "information" etymologically comes from Latin *informatio* which means representation, image, outline, conception [Kumaniecki 1996]. It is an ambiguous term, because it functions in colloquial language and numerous areas of science. These facts cause many problems with providing its definition. Depending on the context and scientific field we may distinguish its various meanings influenced by different perception of reality in each case. It is difficult to indicate a definition which meets the needs of at least several areas of social life [Stefanowicz 2004; Gomółka 2000; Wiener 1961].

Another definition, which has been accepted by the OAIS (Open Archival Information System) and used by NASA, should also be mentioned. According to this definition information is any type of knowledge that can be exchanged, regardless of its form of expression/representation (physical, digital). In compliance with this approach data are forms of representation in reference to a specific piece of information. Thus, access to information is feasible for the recipient who has data and interprets them according to the rules associated with a given form of representation [Reich & Sawyer 1999].

According to the ISO/IEC 27002:2013 standard information is defined as an asset valuable for a given institution, hence, should be properly protected [ISO/IEC 27001:2013]. Moreover, in ISO/IEC 27002:2013 there are many forms information can be expressed in:

- printed,
- written,

- electronic,
- audio and video,
- oral.

Information security is a term located at the edges of technology, organization and law. Guidelines related to the ISO/IEC 27002:2013 information security management system define this term as retaining three features of information: confidentiality, integrity and availability. The standard also takes notice of retaining the following characteristics: accountability, authenticity, non-repudiation and reliability as well as legibility, survivability, functionality, performance and comprehensibility. Among the features enumerated above the first three [Stokłosa, Bilski & Pankowski 2001] amount to the basis of the Information Security Management System understanding of the essence of information security. The significance of individual features depends on circumstance, e.g. in the case of data stored on tapes it is survivability and in reference to a lecture in a foreign language the key characteristic is comprehensibility.

The ISMS certificates become increasingly popular; in December 2012 in 103 countries there were 19,577 certified information security management systems registered (in 2011 in 100 countries there were 17,355 ISO/IEC 27001 certificates) [The ISO Survey 2012].

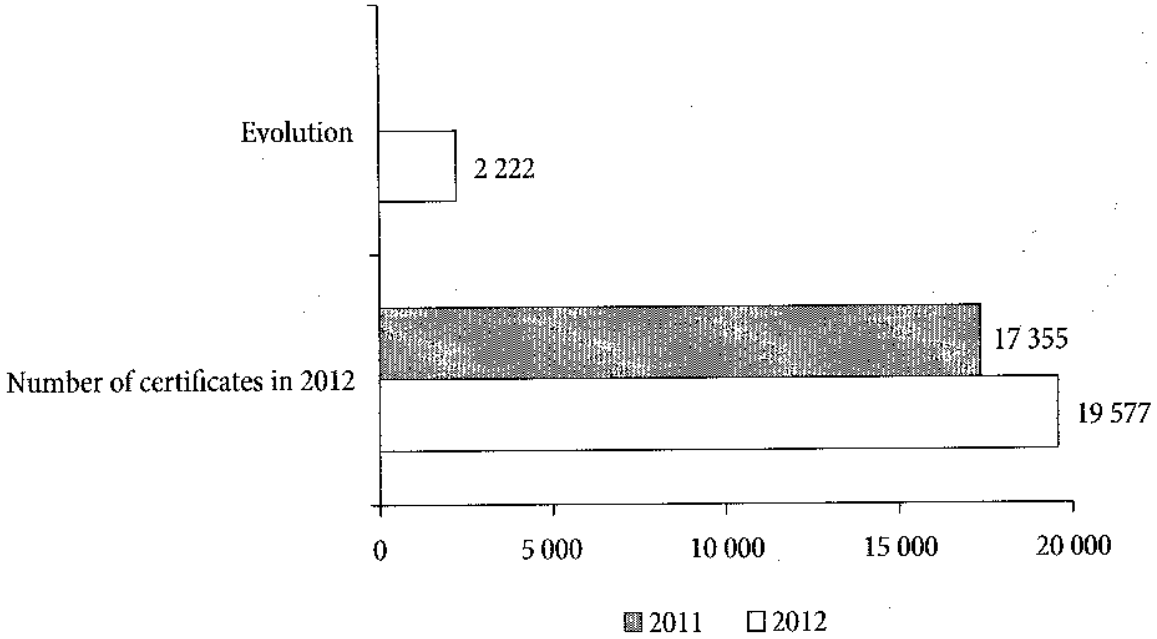

Figure 13. Number of ISO/IEC 27001:2005 certificates in the world in 2011 and 2012

Source: On the basis of ISO Survey 2012

The leading countries in the context of applying the ISO/IEC 27001 standard are Japan, the United Kingdom and India (Figure 14). The popularity of the standard in Japan may be explained by the fact that the Japanese legislation indicates the ISO/IEC 27001 (formerly BS 7799–2:2002) as a benchmark in some areas of business.

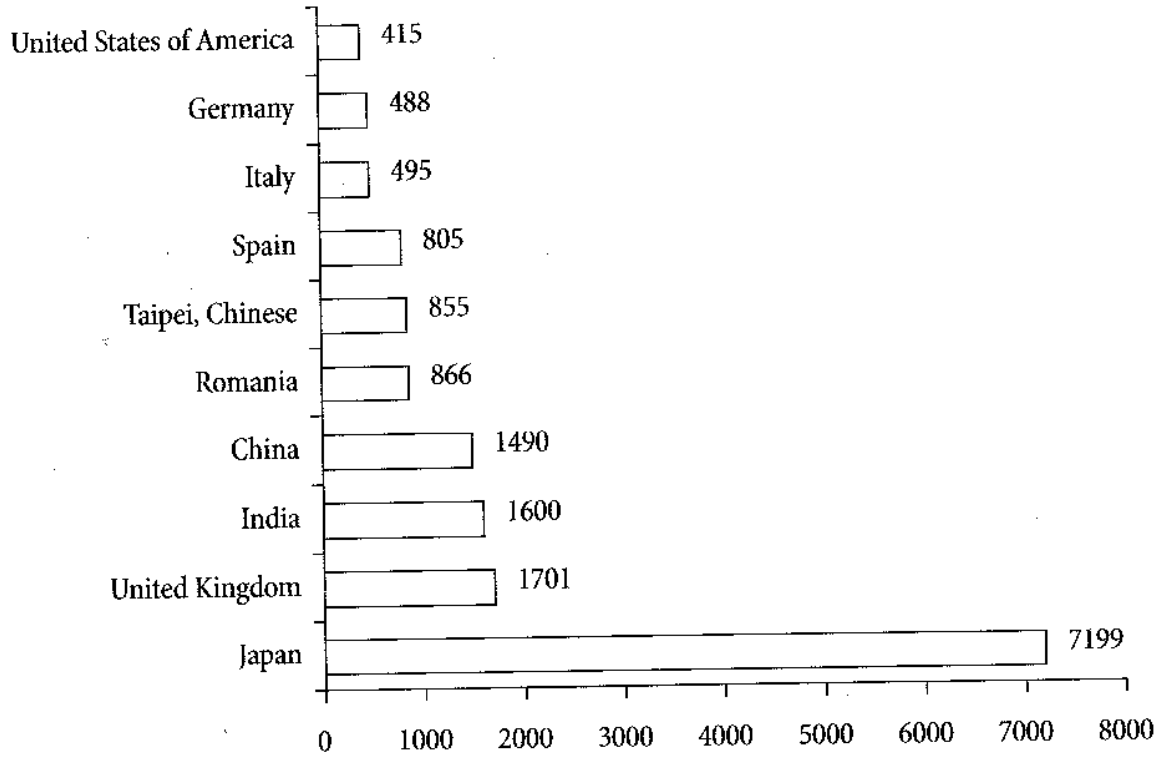

Figure 14. Ten countries with the biggest number of ISO/IEC certificates (2012)

Source: On the basis of ISO Survey 2012

Definitely the most visible increase in the number of certified information security management systems occurred in Romania, Japan and China, as these countries are at present extremely attractive locations for numerous IT specialists, call-centers and IT services, but also in the United Kingdom, India, Spain, the United States of America, Bulgaria and Holland.

Until the end of 2012 in Poland there were 279 ISO/IEC 27001 certificates [www.ISO27001.pl]. The number of conducted accredited certifications was hitherto relatively small, however, we may observe an increase in the number of issued certificates in the world as well as growing popularity of ISMS trainings and certification inquiries in Poland.

2. Conception of the Information Security Management System [ISO/IEC 27001]

The culmination of actions taken by ISO within the scope of unifying the requirements associated with systematic information security management is the ISO/IEC 27001 standard published in 2013. This standard was created in cooperation with JTC-1 (Joint Technical Committee – Information Technology) and, in principle, allows integration with other modules of normalized management systems, e.g. ISO 9001, ISO 14001 [ISO/IEC 27001:2013]. Therefore, a single properly designed system may be in compliance with numerous standards.

The ISO/IEC 27001 standard requirements were grouped in the following chapters:

- Information security management system,
- Leadership and commitment,
- Internal audit,
- Management review,
- Improvement.

The ISO/IEC 27001 standard amounts to an ISMS model which may be applied by any organization, regardless of the specificity of its activity, size, realized processes, legal status and organizational structure. This model allows establishing, implementation, exploitation, monitoring, reviewing and improvement of the management system. The ISMS implementation should be perceived as a strategic decision and ought to stem from business needs of a given organization. Solutions used in the frames of an ISMS should be adequate to the organization's needs.

The decision about implementation of system based on the ISO/IEC 27001 standard does not allow exclusion of any of its requirements [ISO/IEC 27001:2013]. It is possible, though, to exclude selected controls on condition that the risk acceptance criteria are met – the exclusion should be well-grounded, documented and confirmed. Such a situation must not lower the security level in the organization or prevent meeting the requirements stemming from risk assessment, legal regulations and the ISO/IEC 27001 standard.

The source of the model approach to information security management is the aforementioned ISO/IEC 27001 standard. The standard presents requirements related to information security management in organizations. The set of the latest practical requirements, Information Technology – Code

of practice for Information Security Management, published in 2005 supplements the standard.

The ISO/IEC 27001 standard defines individual elements of controlling and monitoring information security. The elements are divided into 10 groups of requirements which allows the organization to identify the most appropriate controls in the context of its specificity, market environment and needs. Particular emphasis is put on risk management. The standard refers to all forms of information, including oral, graphic as well as to the infromation created with the use of mobile phones or fax machines. The standard embraces the latest forms of economic activity, e.g. e-commerce, Internet, outsourcing, teleworking, mobile computing. Below there is a brief description of separate chapters provided.

Security Policy
Policy is the most important document in the information security management system. It creates guidelines and frames for the remaining rules. This part describes relevant tips for an organization which should be taken into consideration during the development of information security policy.

Organization of Information Security
Creating rules of protecting information does not guarantee establishing the system yet. In order to do so it is necessary to appoint proper structures for management inside the organization. It is also significant to identify external companies with the access to information and define appropriate methods of supervision over third parties.

Asset Management
The verification of information processed and stored in the organization is necessary. As a result of information classification groups are created. Moreover, the rules related to these groups are described.

Human Resources Security
The most vulnerable elements of every system are people. The standard demands supervision over separate groups of employees: potential candidates, trainees, new employees, employees expected to be promoted. It is necessary to create a system of trainings and raise employees' awareness of risks.

Physical and Environmental Security
This point describes requirements related to physical protection of buildings, utility rooms and server rooms. It is also necessary to describe the rules linked with appliance maintenance, including computers, and define the needed workplace culture, e.g. clean desk policy.

Communication and operation security
Many mistakes related to information security are caused by misuse of appliances. That is why it is necessary to create rules of using given appliances, including the equipment owned by external companies. Viruses and other dangerous software amount to a significant threat. In order to avoid valuable electronic data it is crucial to establish rules of creating backup copies and managing them. Another important element is using portable data storage devices in a safe way and developing rules of information exchange with third parties.

Access Control
Computer systems include enormous amount of data. It is necessary to control the access to the data by establishing clear users groups and defining authorization to edit and read. This is relevant to information accessible via internal and external networks. Access control should begin at the level of operating systems.

Information Systems Acquisition, Development and Maintenance
While developing an information system controls should always be taken into account. Every change must be authorized and before implementation tested in selected testing environment. This part also describes safe ways of using cryptographic methods.

Information Security Incident Management
Reporting, registering and reacting to all incidents related to information security are the key elements of an information security management system. Systematic communication solutions inside the company, indicating people responsible for reacting to incidents, defining communication paths and maximal reaction time (in reference to incidents) guarantee the efficiency of the ISMS and become the basis for precise risk level assessment.

Business Continuity Management
Each organization should take appropriate measures in order to assure continuity of the most important business activities. These measures embrace the analysis of the most probable and severe failures as well as they include creating plans which are designed to rapidly restore the company to proper functioning. Furthermore, the plans must be periodically tested for utility in emergency situations when the threats materialize.

Compliance
The basic condition of certifying an information security management system is full compliance with present legal regulations. In order to meet the require-

ments included in the standard it is necessary to analyze legislation within the scope of information security and introduce solutions which guarantee full obedience to the law. In addition, it is crucial to introduce certain instruments, e.g. internal audits, leadership reviews, which improve the information security system.

A significant characteristic of the standard is combining potential external threats, commonly acknowledged as the most dangerous, with the analysis of external threats. It means that according to the standard not only market partners, suppliers and recipients may amount to potential threats to economic information, but also external threats linked with employees are important.

The model of the system should be conformed to process approach. In practice there is a necessity to use the philosophy embraced in the Deming circle (PDCA), and in the case of systems integrated with quality management systems it is essential to take account of information security management in the structure of processes resulting from the QMS (ISO 9001).

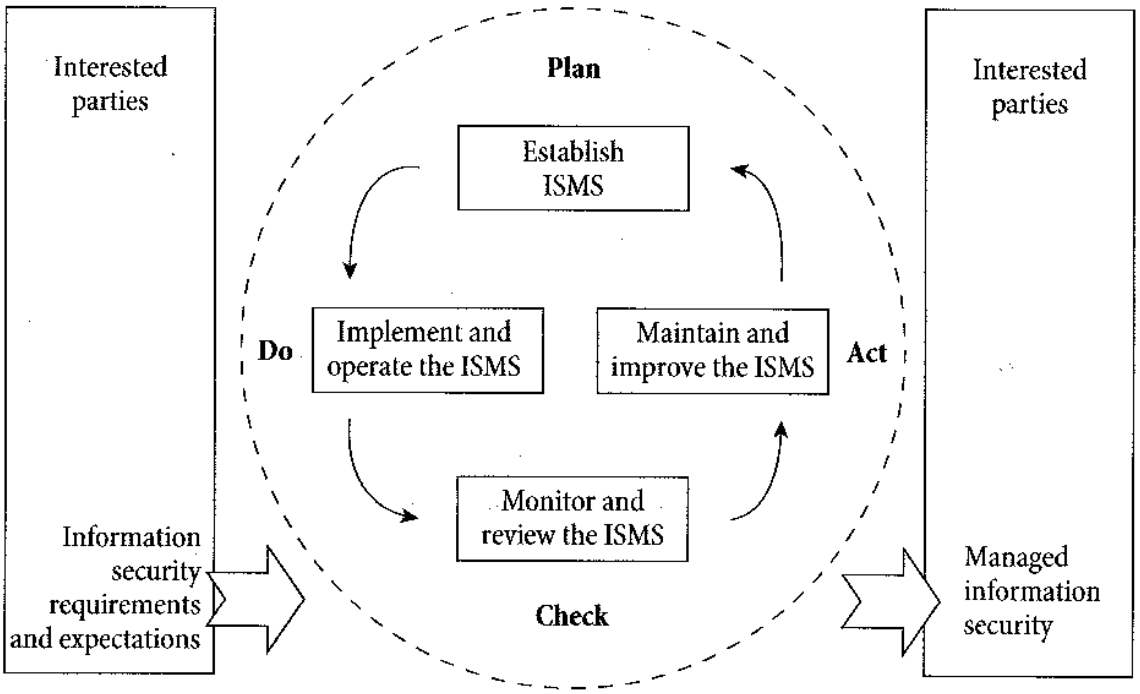

Figure 15. PDCA model used in ISMS processes

Source: [ISO/IEC 27001:2013]

Process approach becomes particularly significant in the face of:

- understanding information security requirements in the organization and establishing information security objectives,

- implementation and exploitation of controls in order to manage information security risk in the context of the organization's total business risk,
- monitoring and reviewing efficiency and effectiveness of the ISMS,
- constant improvement on the basis of objective measurement.

The ISO/IEC 27001 standard, in spite of requirements associated with creating, functioning and maintaining the information security management system, defines objectives and controls. The complete list of requirements in this regard may be found in Annex A. The relevant part of Annex A consists of 11 chapters numbered form A.5 to A.15. This type of numeration stems from the structure of ISO/IEC 27002 which is a set of good practices in information security and information security management systems.

In order to assure better legibility of the present part of the handbook the ISO/IEC 27002 (Annex A) numeration was retained.

A.5. Security Policy
A.6. Organization of Information Security
A.7. Asset Management
A.8. Human Resources Security
A.9. Physical and Environmental Security
A.10. Communications and Operations Security
A.11. Access Control
A.12. Information Systems Acquisition, Development and Maintenance
A.13. Information Security Incident Management
A.14. Business Continuity Management
A.15. Compliance

The order in which security areas are included in the standard does not carry any information about their importance for the information security management system. All areas are equally significant. They consist of 39 objectives in which controls are indicated along with tips for realization and other technical or legal information.

Each security area (A.5, A6,...) consists of separate security objectives (A.5.1, A.6.1,...). Security objectives are supposed to show expected achievements. Each security objective must include at least one control (A.5.1.1, A.5.1.2,...), i.t. one specific means to attain a given objective.

Security objectives as well as controls included in them are enlisted in Annex A and do not exhaust the subject of information security. Annex A should be treated as the absolute minimum in reference to information security management. Thus, the organization may decide to introduce additional controls and security objectives.

Table 6. Structure of Annex A

Security area	Number of security objectives	Number of controls
A.5. Security Policy	1	2
A.6. Organization of Information Security	2	11
A.7. Asset Management	2	5
A.8. Human Resources Security	3	9
A.9. Physical and Environmental Security	2	13
A.10. Communications and Operations Security	10	32
A.11. Access Control	7	25
A.12. Information Systems Acquisition, Development and Maintenance	6	16
A.13. Information Security Incident Management	2	5
A.14. Business Continuity Management	1	5
A.15. Compliance	3	10
Total	3	133

Source: Own research.

3. Establishing and Managing the ISMS

Applying the ISO/IEC 27011 standard is not obligatory, but in the case of positive decision to implement and certify an information security management system it is necessary to establish, implement, exploit, monitor, review, maintain and improve the documented system in reference to the activity and risk of a given organization [ISO/IEC 27001:2013]. Hence, all requirements need to be deeply analyzed; it is not enough to treat them declaratively as it is crucial to provide evidence for their application. If required it is necessary to document solutions and it is always obligatory to verify their adequacy, sufficiency and effectiveness. The key to design optimal implementation of an ISMS is to base it on the results of risk assessment.

At the stage of implementation, maintenance and development of the system it is necessary to [ISO/IEC 27001:2013]:

- define the scope and borders of the ISMS;
- define information security policy;
- define the method of risk assessment and its application, analysis and risk evaluation;
- define and evaluate variations of risk treatment;

- define objectives related to controls treatment and controls, understood as means of risk treatment;
- receive approval for residual risk;
- receive confirmation of leadership for the ISMS implementation and maintenance;
- produce the Statement of Applicability;
- realize all the elements (established in the face of the standard's requirements) of the ISMS stemming from the ISO/IEC 27001 requirements.

Each organization may design its own individualized ISMS based on any model; however, in the case of choosing the ISO/IEC 27001 standard and intending to receive the certificate it is necessary to meet all requirements. It is acceptable to exclude some controls, however only on aforementioned conditions. The scope of the ISMS must be established, i.e. the organization must establish processes, organizational structures, departments etc. embraced by the system.

During defining security policy, the leading ISMS document, it is crucial to assure proper description of the organization's activity, specificity, location, assets and technology.

The content of information security policy, no matter how original, must [ISO/IEC 27001:2013]:

- include frames for establishing objectives; show a general direction and operating procedures related to information security;
- embrace business, legal and regulatory objectives as well as contract commitments associated with security;
- establish strategic context of risk management in the organization which creates room for establishment and maintenance of the ISMS;
- define criteria according to which risk should be assessed.

The content of security policy must be confirmed by the leadership.

Another significant requirement of the ISO/IEC 27001 standard is defining the risk assessment approach in the organization [ISO/IEC 27001:2013]. In this regard it is essential to:

- indicate the risk assessment method, relevant to the ISMS; define information security in the context of the organization's activity as well as legal and monitoring requirements,
- develop criteria of risk acceptance and define the acceptable risk level,
- select the risk assessment method which should assure that the assessment results in comparable and consistent results[38].

[38] Authors stressed the fact that the risk assessment method may be selected from numerous and easily available methods or it can be created as a new individualized method on condition that its effectiveness and results comparability are proven. ISO/IEC 27001 indicates

Next risk assessment is required through [ISO/IEC 27001:2013]:
- defining assets embraced by the ISMS scope and their owners[39],
- defining risks for these assets,
- defining susceptibility which may be used by threats,
- defining results of the loss of confidentiality, integrity and availability in relation to given assets.

Another step required by the standard is linked with the necessity to conduct the analysis and assessment of risk. In this context it is essential to [ISO/IEC 27001:2013]:
- estimate damages and business losses in the organization which may be the result of security violation (potential consequences of the loss of assets' confidentiality, integrity and availability must be taken into account),
- estimate real probability of security violation in light of significant threats and susceptibility as well as consequences associated with assets and recently implemented controls,
- define risk levels,
- decide whether the risk is acceptable or calls for action (with the use of accepted criteria).

Another necessity related to meeting requirements is to identify and evaluate variations of risk treatment. The options in this regard include [ISO/IEC 27001:2013]:
- application of proper controls;
- exploring and accepting risks in a conscious and objective way, provided that they clearly meet conditions (defined in the organization's policy) and risk acceptance criteria;
- avoiding risks;
- transferring business risks to other participants, e.g. insurers, suppliers.

It should be remembered that the minimal set of controls was presented in Annex A of the standard [ISO/IEC 27001:2013]; all the controls should be applied. In addition, it is more important to achieve objectives related to information security. Hence, if the planned security level is assured, it is possible to exclude some controls (achieving objectives – assuring the system's

that there are various risk assessment methods. Some examples of them are provided in ISO/IEC TR 13335-3, Information technology — Guidelines for the management ol IT Security — Techniques for the management ot IT Security.

[39] See ISO/IEC 27001, p. 11. The term "owner" describes a person or subject with defined leadership responsibility for monitoring production, development, maintenance, application and security of assets. This term does not mean that this person has any ownership rights in reference to the assets.

effectiveness). The selected and applied controls must be defined in the ISMS specific document – the Statement of Applicability.

Furthermore, while coping with risk we may exclude it from the organization and its processes. A good solution in this regard is technological and outsourcing processes, e.g. maintenance, human resources management, document archiving. Realization of processes, or just selected actions outside the organization, is possible to some limited extent and it should be remembered that such a conception creates new risks associated with external contractor, external communication, transportation etc. The necessity to transfer risks to other participants stems from the abovementioned arguments.

Process reorganization is a radical action which eliminates given risks. For example, resignation on a given process, action or even technology in order to exclude a specific risk. It sounds incredible, but becomes real when we compare objectives, threats, susceptibility and it turns out that risks amount a threat to the organization's vital interests.

Another requirement of the ISO/IEC 27001 standard is the necessity to select objectives linked with controls treatment and controls (understood as means of risk treatment). The Statement of Applicability is the sign of meeting this requirement, but it has to be produced in relation with the security policy content.

Controls objectives and controls should be selected and implemented in a way that they meet requirements identified and implemented in risk assessment and risk treatment processes. The selection should take account of risk acceptance criteria as well as legal requirements, monitoring requirements and contract commitments [ISO/IEC 27001:2013].

According to the valid rule objectives and controls included in Annex A of the ISO/IEC 27001 standard do not amount to their sole source, but should be treated as merely the absolute minimum which should be selected as a part of this process in order to properly meet the identified requirements. Depending on the organization's specificity some additional objectives of controls treatment and controls may be selected.

As a result of planned and realized activities associated with risk treatment (since the realization of these actions is based on the Deming circle) there are some new residual risks. Therefore, it is necessary to obtain the leadership's acceptance for their level [ISO/IEC 27001:2013].

Next essential measures (requirements) of the standard are obtaining the leadership's authorization to implement and apply systematic solutions as well as preparation of the Statement of Applicability [ISO/IEC 27001:2013]. The Statement of Applicability is the most specific document of the IMSM which must include:

- controls objectives and selected objectives as well as relevant justification,
- already implemented controls objectives and objectives,
- information about exclusion of any control objective and control enlisted in Annex A along with the justification for exclusion.

It is obvious that the content of the Statement of Applicability amounts to the culmination of actions associated with risk treatment. The justification for exclusions enables another check if any threat has been deliberately omitted.

4. ISMS Implementation and Application

Within the scope of actions described in the ISO/IEC 27001 standard as implemented and applied solutions of the ISMS it is necessary to [ISO/IEC 27001:2013]:

- formulate a risk treatment plan which includes leadership actions, areas of responsibility and priorities for information security risk management;
- implement a risk treatment plan in order to achieve identified control objectives which embrace roles assignments and areas of responsibility;
- implement controls defined in SoA so as to achieve objectives associated with their application;
- define methods of measurements and effectiveness associated with controls (and groups of controls) as well as indicate the measures which should be applied during control effectiveness assessment[40];
- implement awareness programs and trainings;
- manage solutions established in the frames of the ISMS as well as its resources;
- implement procedures and other effective controls in order to immediately detect and react to incidents associated with security violation.

These general requirements define strategic directions of the activities in the ISMS. The requirements refer directly to establishing and implementing the system, indicate specific conceptions (e.g. SoA), describe preparation and implementation of the risk treatment plan along with relevant areas of responsibility.

It is typical of international standards to provide general definitions of requirements. In this case it is necessary to plan and realize activities related to risk treatment, however, it may be one specific document based on risk assessment report or various studies which exhaust this subject. Typically these are areas of responsibility and employee authorization associated with

[40] In order to achieve consistent results.

information security, procedures developed within the scope of the ISMS, business continuity plans etc.

Another important requirement refers to implementation of controls defined in the Statement of Applicability as well as is linked with the necessity to monitor the effectiveness of these controls. It is a "new" element which in practice causes many problems. Actions in this regard vary, but most frequently boil down to typical tools of the ISMS – incident management, audits, monitoring, controls, effectiveness evaluation of trainings, but also specific measures related to given controls. It should be remembered that only adequate actions associated with risk treatment may be seen as properly defined. In reference to risks, which slightly exceed the marginal level of risk, standard controls may be applied, however, in relation to key risks the controls must be particularly well-suited. Therefore, it is necessary to define priorities of information security risk management.

Risk treatment management should embrace varied activity which increases its effectiveness.

5. Monitoring and Reviewing the ISMS

Within the scope of the information security management system it is required to monitor and review the system. The organization must realize monitoring and reviewing procedures as well as other controls in this regard so as to [ISO/IEC 27001:2013]:

- immediately detect errors in the processing results;
- immediately identify failed security violations and incidents;
- enable the leadership statement if the information security actions delegated to individuals or implemented with the use of IT resources are realized in accordance with expectations;
- support the process of security violation detection, i.e. prevent security incidents with the use of measures;
- determine if the actions taken in order to solve security violation problems were effective.

Moreover, it is necessary to:

- conduct regular effectiveness reviews of the ISMS (including compliance policy in reference to the ISMS objectives as well as controls review) taking account of the results of security audits and effectiveness evaluation, incidents, suggestions and feedback from all participants;

- evaluate the effectiveness of controls in order to verify their compliance with security requirements;
- review risk assessment, residual risks and risk acceptance levels at planned intervals taking account of changes in the organization, technology, business and process objectives, identified threats, effectiveness of implemented controls, external occurrences (e.g. changes in the law, relevant regulations and the society, changes stemming from contract commitments);
- conduct internal audits of the ISMS at planned intervals.

Furthermore, it is essential to plan and realize, at planned intervals, the ISMS reviews by the leadership. The aim of management reviews is the verification of the ISMS scope and determining potential changes. In addition, security plans should be updated on the basis of the results of monitoring and verification of the scope as well as effectiveness of systematic solutions.

It is required to register activities and occurrences which may influence the effectiveness and efficiency of the ISMS.

6. Maintenance and Improvement of the ISMS

An organization which applies for or owns a certificate of the information security management system must take the following measures [ISO/IEC 27001:2013]:

- implement identified improvements in the ISMS;
- take appropriate corrective and preventive actions;
- draw conclusions from the organization's experiences in the area of information security (as well as from other organizations' experiences);
- inform all interested parties about actions and improvements at the proper level of comprehensiveness and, if needed, determine future actions;
- assure that improvements achieve planned objectives.

7. Risk Management in Information Security

Information systems consist of resources that should be protected (it applies to both internal and external resources). All resources have certain susceptibilities which may be used by threats. The risk in this case may be defined as

probability of undesirable use of susceptibility. In order to minimize the risk controls (procedures, good practices, physical protection, software protection, risk reduction mechanisms etc.) are applied. However, using any of them does not guarantee information security as there always remain residual risks. It may also turn out that a susceptibility has no threat that it could be used by. This situation means that such a susceptibility does not need to be protected by specific controls (but may be). Whitman and Mattord depict risk factors (Figure 16) [Whitman & Mattord 2006].

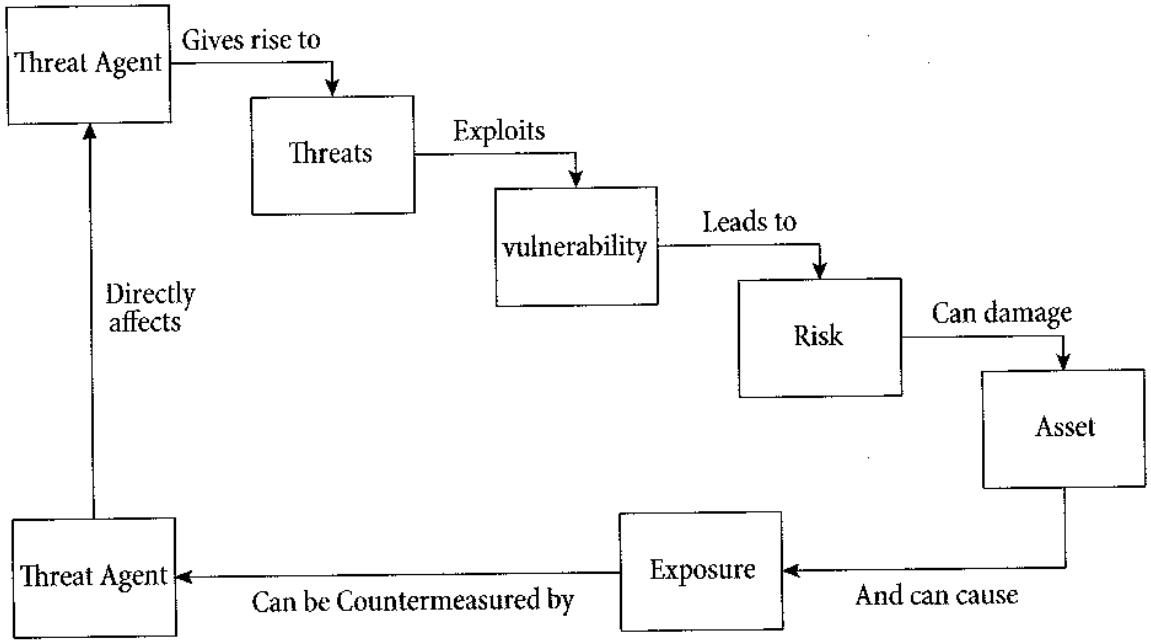

Figure 16. Relations within the scope of risk factors

Source: On the basis of [Whitman & Mattord 2006]

A comprehensive and constant process leading to creating and maintaining security in an institution is called management system. It consists of many subprocesses among which risk management may be found. The key element of risk management is risk analysis. This division in presented in Figure 17 [Alberts & Dorofee 2003].

The ISO/IEC 27002 standard defines risk as the probability that a particular threat will use the susceptibility of a resource or a group of resources in order to cause losses or damage of the resources [ISO/IEC 27002:2013]. Susceptibility of a resource should be understood as weakness of a resource or a group of resources which may be used by the threat [ISO/IEC 27001:2013].

Risk, understood in the way explained above, may be defined as the product of probability (frequency) of an occurrence and the size of the losses incurred

by the occurrence or the value of the asset. In accordance with such an approach the risk is identical when the probability of an undesirable occurrence is insignificant, but losses are big, and when the probability is big, but potential losses are insignificant in terms of business activity.

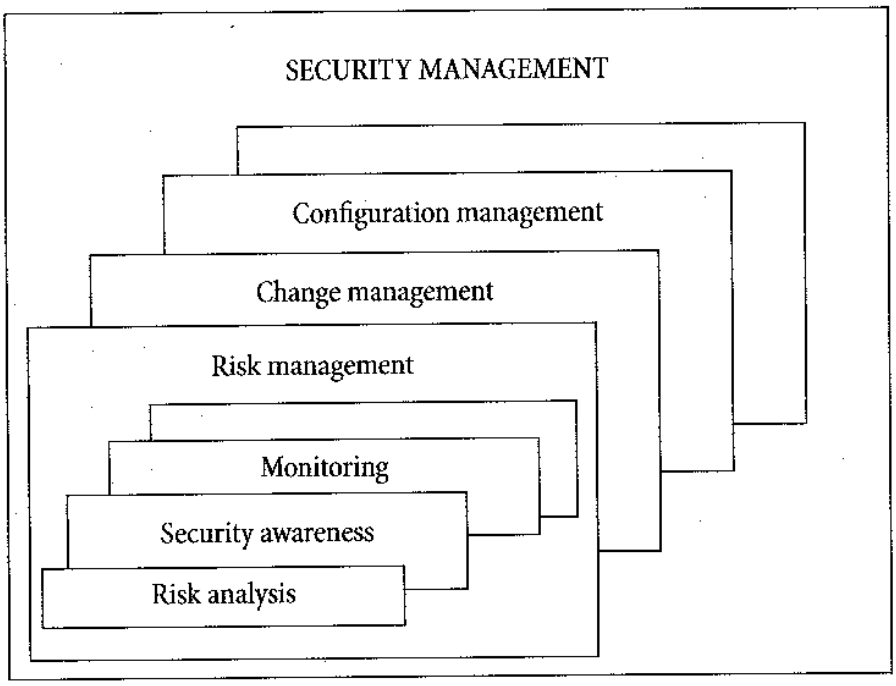

Figure 17. Risk management

Source: [Alberts & Dorofee 2003]

Thus, (information) security management is a set of complex relations including among others: risk analysis, awareness, monitoring the effectiveness of controls, risk management, modifications and configuration.

Risk management is a process of risk assessment which aims at limiting the risk to an acceptable level. It should consist of the following stages: planning, acquisition, development, testing, proper distribution of information systems [Molski & Łachota 2007].

According to Zoła [http://kni.kul.lublin.pl] it is a comprehensive process of identification, monitoring and elimination or minimizing the probability of uncertain occurrences which may influence the resources of an information system. Risk analysis is a process of identifying risk, determining its size and areas which need to be protected.

Whitman takes notice of mutual relation between risk assessment and its decrease – the essence of risk management [Whitman & Mattord 2006].

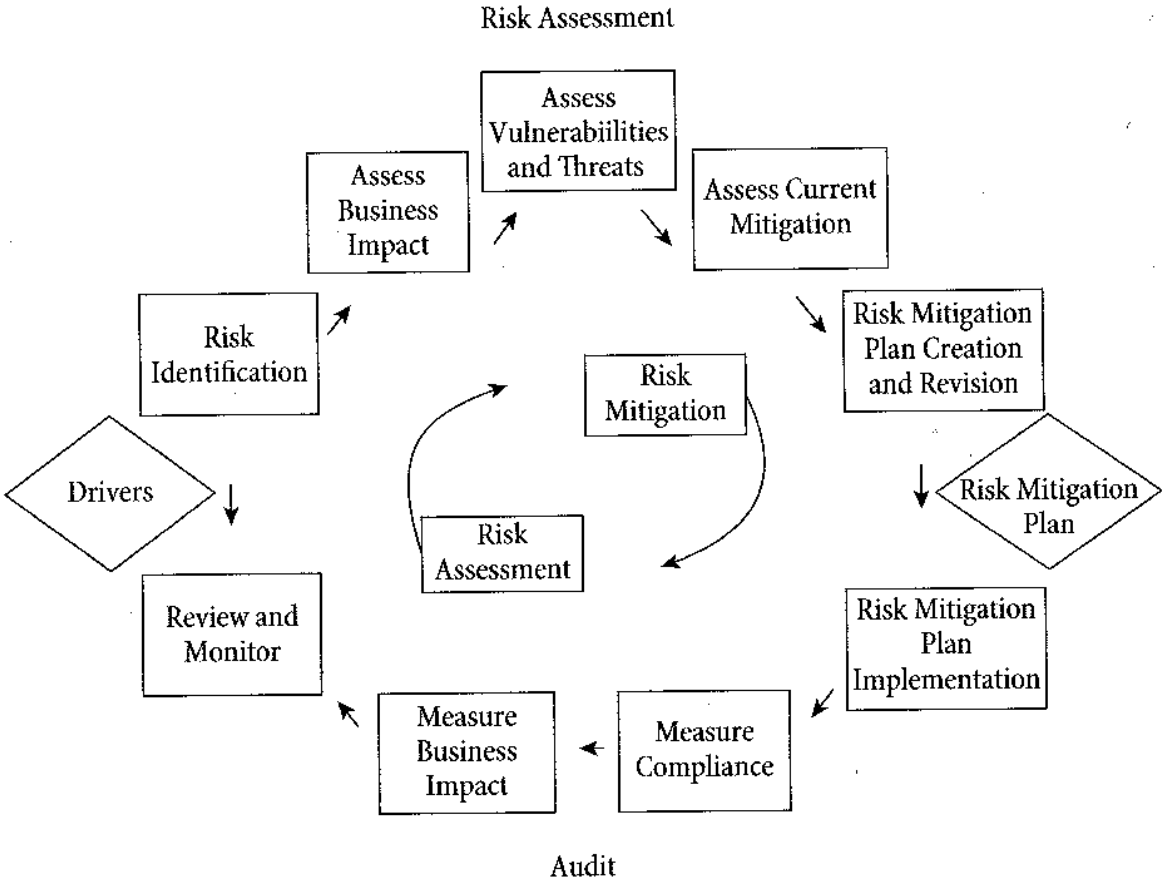

Figure 18. General structure of risk management in the ISMS

Source: On the basis of [Whitman & Mattord 2006]

Whitman [Whitman & Mattord 2006] indicates separate stages of risk management:

- risk identification,
- business impact assessment,
- assessment of vulnerabilities and threats,
- current mitigation assessment,
- risk mitigation plan creation and revision,
- risk mitigation plan implementation,
- compliance measurement,
- business impact measurement,
- revision and monitoring.

In compliance with the ISO/IEC 27002 standard [ISO/IEC 27002:2013] risk management is understood as a comprehensive process of identification, monitoring and eliminating or minimizing the probability of uncertain occurrences which influence the resources of an information system [ISO/IEC 27002:2013].

This approach is also illustrated by Alberts and Dorofee with the use of a modified quality circle (PDCA).

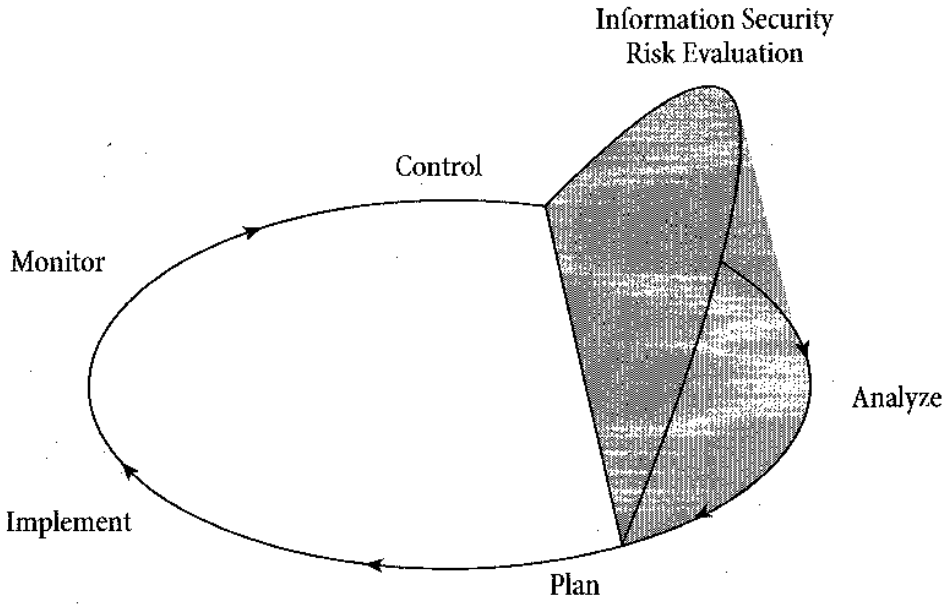

Figure 19. Risk evaluation in information security risk management

Source: [Alberts & Dorofee 2003]

In model approach the aim of the risk management process is to limit the risk to an acceptable level of risk with an appropriate risk treatment plan. The assumption included in the model is that the actions realized with it are effective and done in a constant and systematic way (monitoring, reviews).

Whitman and Mattord describe risk management process in the following configuration: categorization – assessment – communication (Figure 20) [ISO/IEC 27002:2013].

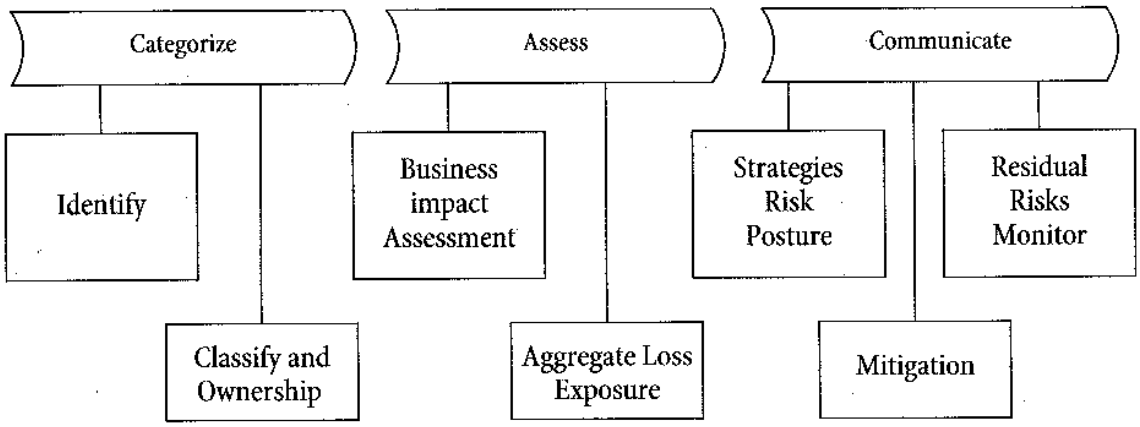

Figure 20. Management risk process

Source: [Łuczak & Tyburski 2010]

Whitman and Mattord also take notice of that the lack of properly defined and communicated course of a process, risk management becomes a threat hazard.

Corrective action associated with information security must be result-oriented, in no case can the selection of controls be located at the beginning (or the end) of activities. The essence of the information security management system must be risk management independently of the reasons for the ISO/ IEC 27001 implementation (and certification) or a different (own) basis of the system.

References

Alberts, Ch., Dorofee, A., 2003, *Managing Information Security Risks. The Octave Approach*, Addison-Wesley, Boston.

Gomółka, Z., 2000, *Cybernetyka w zarządzaniu*, Placet, Warszawa.

http://kni.kul.lublin.pl/~andy/ref/other/risk.pdf [access: 20.12.2013].

ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements.

ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls.

Kumaniecki, K.,1996, *Słownik łacińsko-polski*, Wydawnictwo Naukowe PWN, Warszawa.

Łuczak, J., Tyburski, M., 2010, *Systemowe zarządzanie bezpieczeństwem informacji* ISO/ IEC 27001, Wydawnictwo Uniwersytetu Ekonomicznego w Poznaniu, Poznań.

Molski, M., Łachota, M., 2007, *Przewodnik audytora systemów informatycznych*, Helion, Gliwice.

Reich, L., Sawyer, D., 1999, *Archiving Referencing Model*, White Book, iss. 5, CCSDS.

Stefanowicz, B., 2004, *Informacja*, Oficyna Wydawnicza SGH, Warszawa.

Stokłosa, J., Bilski, T., Pankowski, T., 2001, *Bezpieczeństwo danych w systemach informatycznych*, Wydawnictwo Naukowe PWN, Warszawa–Poznań.

Whitman, M.E., Mattord, H.J., 2006, *Readings and Cases in the Management of Information Security*, Thomson Course Technology, Boston.

Wiener, N., 1961, *Cybernetyka społeczna*, KiW, Warszawa.

www.iso27000.pl – rejestr certyfikatów ISO/IEC 27001 w Polsce [access: 10.03.2014].

The ISO Survey of Management System Standard Certifications 2012.