Management Issues of Information Security

Guzun M., Cojocaru I.
Information Society Development Institute,
Republic of Moldova
idsi@asm.md

Ionescu R.
RINA SIMTEX Certification Body,
Romania
office@simtex.ro

***Abstract* — The paper is focused on management approaches oriented towards the design, implementation, maintenance and continuous improvement of an information security management system (ISMS). It identifies the most common information and communication technology threats, that may affect the integrity, confidentiality and availability of information, causing deficiencies in the organization activity. It describes the organizational measures to be taken in order to establish a management system, that could reduce or even exclude the negative impact of attacks on organisation's information systems. Based on the best practices, provided by the family of international standards in security ISO/IEC 27000, an algorithm for implementation of an ISMS at the organization level is proposed.**

***Keywords* — Family of ISO/IEC 27000 standards, Information and Communication Technology, management system, security policy, ISMS audit, ISMS analysis.**

I. INTRODUCTION

The establishment of computer era is one of the biggest scientific and technical achievements, having had a positive impact on all facets of life in the contemporary society. At present, the activity of most organizations depends more than 65% on their information systems [1]. Most resources and information systems, belonging to the organization, are directly connected to security measures: identification of threats to information resources and vulnerabilities that can be exploited by these threats, the development and application of various protection methods and means. Information security is a set of measures, methods, processes (procedures), which protects information resources and as a result, guarantees the efficiency and practical utility of both the technical infrastructure of information systems, as well as data stored and processed by these systems. The need to develop these measures is related to the fact that modern practice of using information systems is characterized by a large number of attacks on information security. An important factor in this regard is the increased accessibility of information technologies by offenders, as well as information systems' attractiveness as potential targets of attacks.

Some of the most common crimes in information security include:

- Unauthorized access or exceeding access rights to certain informaton or databases, aimed at their appropriation, copying, sending to other stakeholders, illegal use etc.
- Unauthorized use of information resources (information and communication technologies), aimed at obtaining certain benefits or causing damage to both information systems or third parties.
- Purposeful change (forgery) of data.
- Theft of money from electronic "Bank-client" systems, unlawful obtaining of property rights.
- Causing damage to the technical means of information processing, transmission and storage.
- DoS attacks – denial of service, in particular - attacks on servers in Internet.
- Spreading viruses and malware to compromise information systems.

These and other threats require a systematic approach, including appropriate technical, organizational and other measures to ensure the integrity, availability and confidentiality of information within the organization.

II. INFORMATION SECURITY MANAGEMENT AT THE ORGANISATION LEVEL

Ensuring information security within an organization becomes an indispensable part of the overall management system and is necessary to achieve organisational policies and objectives. A systemic approach in this area is even more important, when the degree of processes automation is higher and the intellectual component has a substantial weight in the finished product (technologies, "know-how", commercial databases, results of scientific research etc.). The importance of information security increases substantially, when information flows within the organization include state or commercial secrets, other confidential information (bank secrets, medical secrets, intellectual property, personal data, partner companies' secrets etc.). Information security in these areas is regulated by the state legislation, which is translated into policies and internal procedures of the organization, within an information security management system. International standards have a huge importance for establishing security policies of the organization, because these include best practices in the area and can guide the establishment of a harmonious system for information protection. Therefore, the sources of information security policies at the top management level are: 1. legal and regulatory requirements; 2. requirements of international standards and other standards; 3. objective needs of the organization.

Information security policy includes a set of documents, which set out the basic requirements for ensuring the protection of information and means for practical implementation of these requirements. To develop an information security policy it is necessary to design and implement a management system, which must establish clear rules for all hierarchical levels of the organization.

Top management level:

- Formulates and takes attitude toward information security issues, documenting them in the General policy, objectives and action plans in this field, documents that form the basis for middle and lower level policies.
- Establishes an organizational structure, authorities and responsibilities of all functions, which have an impact on information security.
- Provides staff training and education aimed at raising awareness of employees regarding the importance of compliance to the security norms established by legislation, standards, internal rules of the organization, establishes and applies disciplinary process in cases of violations of these rules.

Middle management level:

- Establishes organisational approaches in certain aspects of information security, setting the roles and responsibilities realated to security in administrative and operational processes of the organization.
- Establishes detailed requirements on information flows and systems in terms of integrity, confidentiality and availability of information.
- Is responsible for compliance with security requirements in developing information and communication technologies.

Lower level management responsibilities refer to particular elements of information systems, sectors and systems for information processing and are described in instructions and specific forms regarding performed activities.

Hierarchical levels and documents that set responsibility and authority in the field of information security are presented in Figure 1.

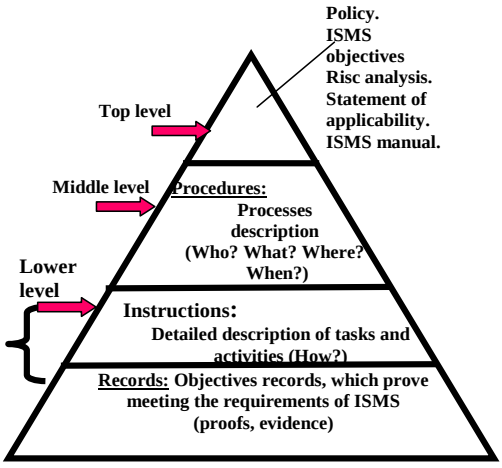

Fig.1. Hierarchy of activities within an Information Security Management System and ISMS documents.

International standards aim to provide a methodological support for organizations which plan to implement, maintain and continuously improve an information security management system, and if necessary demonstrate to interested parties the functionality of the system or ensure the certification of the system by an authorised body. Below is presented a brief description of the family of International Standards ISO/IEC 27000, covering different aspects of information security management.

ISO/IEC 27001 - *Information technology - Security techniques - Information security management systems - Requirements* [2]. Standard edition of 2005 was completely revised in September 2013. The present edition is structured, so that it can be easily integrated with other management systems ruled by ISO standards, such as quality management system, environmental management, health and occupational safety etc.

In this case the procedures for control of non-conformities, document and records control, internal audit, management review will be common for all management systems implemented in the organization. ISO/IEC 27001 is the basic standard upon which the evaluation and certification of an information security management system is carried out.

A family of complementary standards was developed to facilitate the implementation of ISO/IEC:

ISO/IEC 27000:2014 - presents a general characteristic of ISO 27000 family of standards and the vocabulary used in standards.

ISO/IEC 27002:2013 - is a code of best practices in information security, including the ISMS control objectives and security measures to achieve those objectives.

ISO/IEC 27003:2010 - is a guide for the implementation of ISO/IEC 27001.

ISO/IEC 27004:2009 - provides guidance on the application of security metrics.

ISO/IEC 27005:2011 - establishes approaches for assessment, analysis and treatment of security risks.

ISO/IEC 27006:2011 - establishes requirements for certification bodies of information security management systems.

ISO/IEC 27007:2011 - establishes the rules for ISMS audit etc. These standards are supporting the implementation, maintenance and continuous improvement of an ISMS within an organization.

III. ISMS IMPLEMENTATION METHODOLOGY [3].

ISMS implementation is a strategic decision of an organization. By implementing an ISMS the organization can identify the required level of security, develop plans, strategies, can distribute its assets among certain resource holders based on risk analysis and can apply technical and non-technical security measures. The key concept of implementing an ISMS in an organization is focused on improving three attributes of information: confidentiality, integrity and availability.

The implementation process should be organized respecting the PDCA principle. For an effective and efficient implementation of ISMS within an organisation, the following steps should be taken:

ISMS PLANNING

Step 1. Obtaining the agreement and commitment of the top management
This commitment is of major importance for the success of an ISMS implementation project. Commitment must be declared at a meeting with representatives of all hierarchical levels of the organization.
Step 2. Establishing the governance structure of the ISMS. The security structure.
General Director shall establish by a special decison an Information Security Committee and the head of the Committee, which are to coordinate all activities related to implementation, maintainance and improvement of the ISMS.
Step 3. The initial assessment of information security system of the organization. Scope definition.
Any organization, even if it doesn't have a documented and certified ISMS, undertakes certain security measures. The objective of this step is to evaluate the suitability of the existing management system with regard to the standard requirements. This assessment aims to set the context of the organization from the point of view of information security, internal interests as well as those of external parties regarding the ISMS. At this phase the scope of the system is established (processes, locations, activities, applicable/not applicable control measures from Annex A of ISO/IEC 27001:2013). The assessment shall be completed with a report, that matches the current status of the ISMS to the requirements of the ISO standard.
Step 4. Developing ISMS policy statement
The draft policy shall be designed by the Security Committee, taking into account the provisions of p. 5.2 of the standard. It is reviewed and approved by the General Director and circulated to all employees and other stakeholders by means of trainings, its inclusion in the Internal Regulations, website, display panel.
Based on the policy, information security objectives are established within the organization.
Step 5. Completing the inventory of information assets. Classification of assets
The term "asset" refers to all goods within the organization, which must be protected. These include, but are not limited to:

- Infrastructure elements.
- Information and data.
- Paper documents.
- Physical equipment.
- People and their knowledge.
- Image, values, goals, marketing strategy, pricing policy, reputation etc.

Following the completion of information and non-information assets inventory, these resources are classified according to their importance for the organization. The classification will take into account the recommendations offered by ISO/IEC 27002:2013 on classification criteria:

- Legal requirements.
- Value.
- Criticality.
- Sensitivity to disclosure or modification.

At this stage must be established asset owners, who will be responsible for classification, developing measures of asset protection and enforcement of these measures.
Step 6. The approach to risk analysis and management
At this stage the methodology for managing information security risks is defined. When developing the methodology, the recommendations of ISO/IEC 27005:2011 should be followed, which are based on the identification of assets and threats, that can exploit vulnerabilities of the said information assets. The methodology takes into account the impact of loss of confidentiality, integrity and availability of information, as well as the probability of a threat to exploit a vulnerability. The final document of this stage is a risk treatment plan, that will include those responsible for risk management and acceptance of residual risks.
Step 7. Statement of applicability
Following the initial assessment, risk analysis and assets classification, certain security measures to be taken are proposed in the planning phase of ISMS. This document is called Statement of Applicability and contains security measures proposed in Annex A of ISO/IEC 27001:2013, that were selected to reduce the risks calculated in the previous step to an acceptable level. Since not all of the 114 measures are applicable within the organization, some of these may be declared inapplicable (exclusions). In the spirit of the standard, any exclusion is justified in the Statement of Applicability.
Once the Statement of Applicability is completed, the planning phase of ISMS is concluded, which allows the transition to the next stage of the Deming cycle:

ISMS IMPLEMENTATION

Step 8. *Developing the risk treatment plan*
At this stage, the security measures proposed in the planning phase of ISMS are implemented.
Effective application of these measures involves determining the appropriate actions at the management level, resources allocation and definition of responsibilities, that shall lead to complete and correct application of security measures.
Step 9. *Development of the necessary ISMS documents*
The documented information to be developed within ISMS is specified in ISO/IEC 27001:2013 clauses and includes:

- Statement of applicability (clause 4.3).
- Information security Policy statement (5.2).
- Risk assessment procedure (6.1.2.
- Risk treatment procedure (6.1.3).
- Information security objectives (6.2).
- Records related to competence of ISMS personnel (7.2).
- Planning and operational control documents (8.1).
- The results of risk assessment (8.2).
- Risk treatment decisions (8.3).

- ISMS monitoring and measurement records (9.1).
- ISMS internal audit program and audit results (9.2).
- ISMS management reviewe records. (9.3).
- Records of non-conformities and corrective actions taken (10.1).
- Other ISMS documents identified by the organization as required to efficiently operate the ISMS (7.5.1b).

Step 10. *Modifying job descriptions of ISMS employees*

At this stage all job descriptions of employees involved in the ISMS are reviewed by introducing new clauses arising from ISMS documents already developed, such as assets (information goods) under the responsibility of each employee, the risks to be managed by employees, relevant confidentiality clauses and clauses specific to the job. The job descriptions also establish the types of documents/information accessible to each employee. These also specify detailed job descriptions with ISMS responsibilities.

Step 11. *Employees training*

Trainings are critical, because an efficient management system can be successfully implemented only with competent and conscious participation of all employees, having control responsibilities over organization processes. The training must take place at all stages of the project and must ensure that all employees are familiar with the international standard, internal management procedures and external documents related to the activity of the organization.

Step 12. *Effective application of ISMS procedures*

Every employee responsible for a certain process shall apply the documents developed at the previous stages. The application of documents is closely related to the implementation of security measures described in the risk treatment plan.

ISMS VERIFICATION

Step 13. *Periodic review and update of ISMS documents*

One of the purposes of monitoring ISMS implementation is to update the developed documents in order to adapt them to the situation in the organization. This stage includes revisions of documents, withdrawal of old ones and the distribution of corrected versions.

Step 14. *Internal audit*

The common practice for system monitoring is internal audit. It allows to assess the level of implementation of security measures. Internal audit should be performed in all departments involved in ISMS and is carried out through employee interviews, direct observation, systems testing. A necessary component in verifying the implementation of technical measures is the technical audit, which is conducted by qualified personnel with special tools. Internal audits result in conclusions, which are included in internal audit reports (IAR). The findings to be resolved are communicated to the involved parties, as well as the Security Committee and General Director.

Step 15. *Management review (MR)*

Management review is an important step, since by performing a full PDCA cycle, it initiates a new cycle of system development. The review must collect and analyze input data listed in p. 9.3 of the reference standard. It is mandatory to maintain evidence of performing this review. Following MR, ISMS improvement measures must be proposed, resources be allocated if necessary, the risk assessment must be updated, as well as the risk treatment plan if necessary, and eventually procedures and working methods must be improved as well.

SYSTEM IMPROVEMENT ACTIONS

Step 16. *Implementation of MR results*

Following the MR, output data must be implemented in order to improve the ISMS. MR results should also be communicated to and understood by stakeholders. The output data can include both preventive and corrective actions.

REFERENCES

[1] http://ro.scribd.com/doc/99927620/Securitatea Informatională.

[2] ISO/IEC 27001:2013. Information technology - Security techniques - Information security management system – Requirements.

[3] Cojocaru Igor, Guzun Mihail, Ionescu Răzvan. Sistemul de management al securităţii informaţionale ISO/IEC 27001:2013. Algoritmul de implementare. The 8-th International Conference and Computer Science & The 5-th Conference of Physicists of Moldova, Chisinău, Repiblic of Moldova, October, 22-25, 2014, p. 362-365.