IMPLEMENTATION OF SECURITY CONTROLS ACCORDING TO ISO/IEC 27002 IN A SMALL ORGANISATION

MATÚŠ HORVÁTH, MARTIN JAKUB

1 INTRODUCTION

Managerial work is directly dependent on information, it is therefore logical that the success of managerial decisions is directly proportional to the extent and quality of information background. The expansion of computer technology expand also the possibilities in what form information may exist in the organization. Therefore, we use the term asset inside the field of information security (asset ang.), which represents everything that is of value to the organization [1], thus it may be information in the paper (eg a contract), electronic form (eg sales figures) but also services (eg e-mail server organization) or equipment (eg cash register), which are essential for the proper functioning of the organization processes. With protection of information organization's assets and its governance deals Information Security Management System (ISMS). Generally speaking, the ISMS serves to achieve credibility, integrity and availability of organization‘s information assets

ISO / IEC 27001 is international valid standard that specifies requirements for establishment, implementation, monitoring and review, maintenance and improvement of an Information Security Management System. The standard covers all types and sizes of organizations. An organization can be certified to ISO IEC 27001, that enables organizations to assure its stakeholders about the level of information security. Implementation of security controls is one of the key steps in the process of implementing information security management system according to ISO / IEC 27001. Organization responds to security requirements by setting the security controls and thus ensures the security of their information assets. Security controls within organization take the form of guidelines, procedures and measures.

Organization Profile

The area of information security is certainly important also for organizations with few employees. The implementation of security controls in this type of organization is linked with some specifics. In small organizations (up to 20 employees and 2 levels of management) should be the requirements of ISO / IEC 27001 applied, taking into account the possibilities of such organizations (financial and personnel). However it will not change the main goal of the implementation process, the establishment of procedures, rules and system of responsibilities through which an organization can maintain and improve its information security and protect their assets.

The article describes the implementation of security controls in a real organization as one of the key steps. Due to the sensitivity of the information given, we decided not to put a specific name of the organization. The organization operates in the construction industry, focusing on construction work, repairs and capital works in the thermal energy with extension to other areas of construction industry. It is a small-sized organization by number of employees (16 employees and two levels of management). Organization is certified against STN EN ISO 9001:2009 standard. As it is a construction organization, planning and implementation of security controls took place for the project-operational department.

2 SECURITY CONTROLS IMPLEMENTATION

2.1 Security Requirments

At the beginning the whole process of selection and implementation of security controls are the safety requirements set by the organization (Figure No. 1). These requirements may come from several areas. The first and most important area is the output of risk assessment of information security. It is a methodical review of the risks in the organization.

In our case, the risk assessment was carried out by using the method of FAIR (Factor Analysis of Information Risk). This method successively disassembles the risk to partial risk factors that influences its ultimate size and offers the possibility to use the quantitative and qualitative expression of these factors for qualitatively expressing the overall risk.

Tab.1 - Identified hazards and qualitative expression of risk

Threat	Risk
Fire	Critical
Power failure	High
Break-in	Medium
Information theft	High
Internet connection failure	Medium
Organization network failure	Medium
Failure of PC 1	Medium
Failure of PC 2	Medium
Organization e-mail failure	Medium
Hackers attack on organization website	Medium
Computer virus / spyware	Medium
Hackers attack on organization infrastructure	Medium
Hackers attack on organization e-mail	Medium

Another source of security requirements are requirements defined by law, decrees and government regulations. In the case of an organization for which the whole process was carried out, the Law on Personal Data Protection No. 428/2002 and Act about archives and registries 395/2002 were evaluated as relevant requirements.

The third area is requirements arising from contracts and agreements where the other party may impose requirements for confidentiality and security of the information provided. Within the organization the agent identified just one requirement to address information security in contracts with third parties.

The last area is the information security requirements of the practice, resulting from the requirements of current practice in information security in organizations. As the source of these requirements, we used the standard ISO / IEC 27002 Security techniques – Code of practice for Information Security Management.

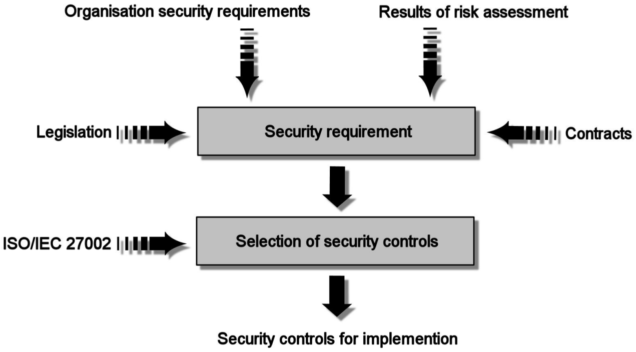
Organisation security requirements
Results of risk assessment
Legislation
Security requirement
Contracts
ISO/IEC 27002
Selection of security controls
Security controls for implemention

Figure 1 - Process of implementation security controls

2.2 Selection of security controls

Based on the identified security requirements is needed to establish such security controls which ensure compliance with security requirements of the organization. The main documents that we used in establishing security controls were standard ISO / IEC 27002. This standard includes guidelines and advices how to implement security controls which are listed in Annex A of ISO / IEC 27001. Annex A of ISO / IEC 27001 standard contains a set of 133 security controls covering general requirements and objectives of organizations in the field of information security.

ISO / IEC 27002 standard also sorts these controls according to the areas in which they operate into 11 groups. Based on the identified security requirements of organizations and systems and technologies used by organization, 88 security controls have been identified that needed to be implemented in the organization. The whole process was documented by a declaration of applicability. Statement on the applicability is required document in standard ISO / IEC 27001 that lists all the controls implemented from the standard ISO / IEC 27002 in the organization.

In our case, this document identified other than the implemented security controls the reason for the implementation (e.g. the outcome of risk analysis). Since ISO / IEC 27001 also requires justification and a record in case when any of the listed security controls in standard ISO / IEC 27002 is not implemented, it contains a statement of applicability and reference to such record. Due to the limited size of article, just a percentage of the implemented and not implemented security controls for each group of security controls from the ISO / IEC 27002 is listed (Fig. 2).

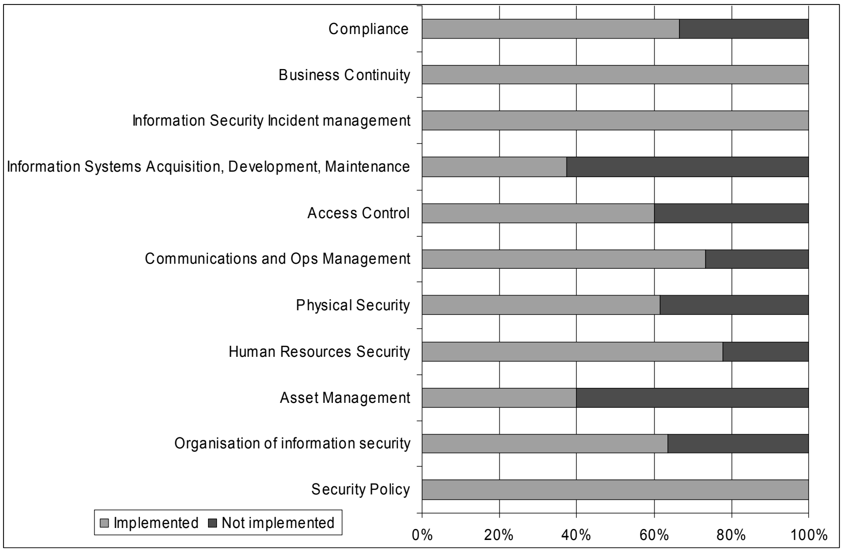

Figure 2 – Implemented security controls across groups

The most common reason for the decision to implement security controls was a requirement arising from the praxis and reaction to the outcome of risk assessment in the organization. (Fig. 3).

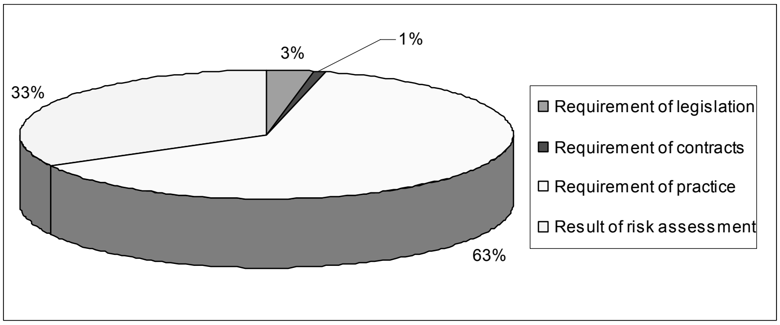

Figure 3 – Reasons for the selection of security controls

2.3 Security controls implementation

ISO / IEC 27001 do not strictly set the form in which it is necessary to implement and document the particular security controls. In our case we implemented the controls through guidelines.

The form of directives we have chosen because of flexibility and easy to use options.

The security guidelines of organizations have been prepared in compliance with the quality manual and therefore they can be easily incorporated within the document management system and system of records in organizations.

During the process, 19 documents were created, meeting the objectives of identified security controls. Established security guidelines cover different fields of information security in the organization through achieving the objectives of security controls in these fields of information security. (Tab No. 2). The only exception is the guideline BS02. FAIR method, which was established under the requirement of ISO / IEC 27001 standard as a supporting guideline for periodic repetition of the process of risk assessment in the organization. All established security guidelines include the following sections.

- Title page
- Purpose
- Scope
- Definitions
- Policies, controls, procedures
- Penalties
- Attachments

2.4 Description of established system

The main security guideline is BS00 - Information Security Management, on the basis of which information security policy and information security objectives are established. Safety guidelines (BS03 - BS15) covers partial fields of information security.

Monitoring the state of information security is carried out by two security guidelines BS16. Monitoring, in addition to general practice, calls for regular review of fulfilling safety principles and controls by employees (at least 1x every 3 months) in field of physical security, information assets, equipment configuration, use of portable media in organization and its content and backup.

Security guideline BS17 - Managing security incidents describes the necessary steps in case of presence or doubt of security incident. State of information security and document management within organization is monitored through internal audits of information security, which are performed in compliance with quality manual. The effectiveness of information security management system is assessed at yearly intervals through the process of management review.

The assessment report is prepared by the agent once per year. Syllabus report consist of:

- Assessment of timeliness of information security policy
- Evaluation of the implementation of the objectives of information security
- Evaluation of implementation and adequacy of resources
- Evaluation of security incidents identified by the previous management eview
- Overall evaluation of information security organization
- Action draft arising from the report

The implemented system uses and respects the organizational structure of the organization documented in the Quality Manual. Organization agent is member of the top management and is also the highest official ISMS of the organization. The agent is also responsible for maintaining the integrity of the ISMS in the organization.

Other responsibilities and powers within the ISMS are listed in specific guidelines of information security. Security manager is responsible for the technical aspects of information security and incident management, while the role takes the software supervisor takes of the organization. Responsibilities and powers of individual employees within ISMS are listed in specific information security guidelines and their violation is considered as causing a security incident.

Tab. 2 Documents created in the organization

Label	**Name of document**	**Number of imple-mented controls**
Document	Information security policy	2
BS00	Information security management	10
BS01	Identification of assets	2
BS02	FAIR method	0
BS03	Physical security and security of environment	5
BS04	Security of equipment	4
BS05	Security of computers	8
BS06	Security of network	4
BS07	Security of communication	6
BS08	Management of access	7
BS09	Third party access	5
BS10	Management of changes	8
BS11	Handling of removable media	4
BS12	Security of personal data	1
BS13	Creating password	1
BS14	Backuping	1
BS15	Operating procedures and training	2
BS16	Monitoring	6
BS17	Managing security incidents	6

3 CONCLUSION

Area infromation security is becoming increasingly critical for any organization. However, for small organizations is the implementation and operation of the ISMS often seen as impossible or very expensive. In this article we have tried to introduce a procedure of one of the key steps in the process of establishing ISMS and its application in terms of small organizations. In many small organizations is not necessary to implement various security controls of ISO / IEC 27002 standard for the simple reason, that the organization doesn‘t use related technology or processes.

Also, the implementation of security controls is not as difficult as in the case of large organizations with many levels of management and various information systems. Further more, integration of ISMS with QMS at the documentation level allows the organization to save on financial and human resources. Also, by delegating the role of security manager to software supervisor, organization can reduce operational system costs. We hope we succeeded in this article to illustrate the real possibility of implementing the requirements of ISO / IEC 27001 even in small organizations at reasonable cost of implementation and operation.

REFERENCES

ISO/IEC 13335-1, (2004) *Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management,* ISO

ISO/IEC 27001, (2005) *Information technology - Security techniques. Information security management systems. Requirements,* ISO

ISO/IEC 27002, (2005) *Information technology -- Security techniques -- Code of practice for information security management*, ISO

Horvath, M, (2009) *Process zavádzania systému manažérstva informačnej bezpečnosti v organizácii,* Ing. Thesis, Košice

ABOUT THE AUTHOR

Ing. Matus Horvath – PhD student at Department of Integrated Management, Faculty of Metallurgy, Technical University of Košice, Slovakia,
matus.horvath@tuke.sk

Ing. Martin Jakub – PhD student on Department of integrated management, Faculty of Metallurgy, Technical University of Košice, Slovakia,
martin.jakub@tuke.sk