INFORMATION SECURITY MANAGEMENT SYSTEMS CERTIFICATION – RESEARCH IN THE ROMANIAN ORGANIZATIONS

Bogdan ȚIGĂNOAIA[1], Anca-Alexandra PURCĂREA[2]

This paper presents aspects regarding some of the international ISO standards in the field of security and the process of certification within an organization of an Information Security Management System – ISMS, according to the requirements from international standard ISO 27001:2013. A research based on a questionnaire regarding this issue was made, the target group of the research were Romanian organizations. The results of this study are highlighted below and final aspects based on the research findings are also presented.

Keywords: management system, information security, organization, research.

1. Introduction and theoretical context

Energy security basics are nowadays at stake, after the Ukrainian crisis [1]. But also the information security in an organization or for a state has at least the same importance in a dynamic society that is today in a continuous transition. According to Pipkin, information security is the process of protecting the intellectual property of an organization [3]. The need of information protection comes from the power mechanism: information is a key factor in taking decisions [4]. The assurance of the information security in companies is an actual and very sensitive subject. There are some mechanisms that can be used in organizations to assure information security such as: cryptographic, biometric, steganographic (an example of a steganographic system can be found in [5]) solutions. There are also a lot of ISO international standards in the field of security, some of them are presented below:

- **Security standards –** Standards from ISO 27k family are the most popular in the field of security assurance.
  - ✓ **I.S.O. / I.E.C. 27000:2014 – Information technology – Security techniques – Information security management systems – Overview and vocabulary** – ISO/IEC 27000:2014 provides the overview of information security management systems (ISMS),

[1] Lecturer , Dept. of Management, University POLITEHNICA of Bucharest, Romania, e-mail: bogdantiganoaia@gmail.com

[2] Professor, Dept. of Management, University POLITEHNICA of Bucharest, Romania

and terms and definitions commonly used in the ISMS family of standards. It is applicable to all types and sizes of organization (e.g. commercial enterprises, government agencies, not-for-profit organizations) [6].

  - ✓ **I.S.O. / I.E.C. 27001:2013 - Information technology – Security techniques - Information security management systems – Requirements** – ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature [6].

- **Other standards:**
  - ✓ **I.S.O./I.E.C. 27006:2011** – Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems;
  - ✓ **I.S.O./I.E.C. 27007:2011** – Information technology — Security techniques — Guidelines for information security management systems auditing;
  - ✓ **I.S.O./I.E.C. 27031:2011** – Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity;
- **Other standards under development:**
  - o **I.S.O./I.E.C. 27016** – Information technology -- Security techniques -- Information security management - Organizational economics;

Regarding organizations, a possible solution for the information security assurance is the implementation and certification of an Information Security Management System according to ISO 27001:2013. It is important to highlight (see Figure 1), in a generic manner, the six steps of the certification process [7]:

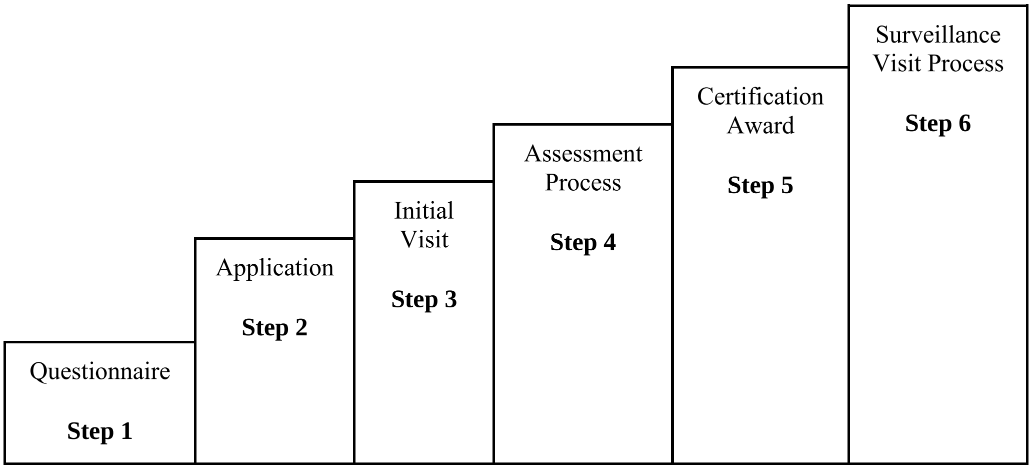


Fig. 1. The six steps of the certification process

Step 1- The organization completes a questionnaire that is sent to a Certification Body – CB, in order to ensure that it is within the scope of the Certification Body's accreditation.
Step 2 - The organization will submit an application for registration with that CB.
Step 3 - Assuming that the quotation is accepted, the Certification Body will carry out the first stage of the audit, an initial assessment of the documented ISMS to determine whether it meets the requirements of the standard [7].
Step 4 - This evaluates the documented ISMS against the requirements of IS0 27001 and reports on any failures at that stage [7].
Step 5 - If the outcome of the conformance audit is successful, then the Audit Team will make a recommendation for certification to the Certification Body [7].
Step 6 - When the ISO 27001 certificate has been granted, a process of periodic monitoring of the ISMS, known as Surveillance Audits, begins. This process is designed to ensure that the organization's ISMS continues to conform to the requirements of ISO 27001 [7].

2. Research in the Romanian organizations

A. Research methodology

In this paper a pilot research has been conducted in order to investigate aspects regarding ISO certification – benefits, the intention of organizations to be certified (in particular for the certification of an Information Security Management System according to ISO 27001:2013 international standard). The target group was consisted of Romanian organizations. In this context, the empirical research has the following objectives:

- To study if the Romanian organizations have an ISO certification, in particular an Information Security Management System;
- To investigate if the Romanian organizations have the intention of such a certification and in this situation, to see the level of knowledge regarding the requirements, benefits and the certification procedure;
- To develop recommendations (possible changes in organizations) in order to outline the importance of the information security assurance and of the implementation and certification of an Information Security Management System in companies.

Variables Measurement

There are two types of variables: nominal scaled and variables regarding Information Security Management Systems. As a summary, Table 1 shows the structure of relevant variables of the research.

Table 1

The map of research variables

Research variables		Conceptual description
Nominally Scaled Variables	Demographic Variables	Gender
		Age
		Professional background
		Organizational characteristics
Variables regarding Information Security Management Systems		Type of certification
		Benefits of certification
		Intention to be certified
		Procedure and requirements to be certified

The qualitative questions were measured using a three point scale (e.g. YES, NO, PARTLY) (adaptation from [2]). The respondents express their general opinion regarding the following items (selection): the type of ISO certification in organizations, benefits of certification, the intention, the procedure and requirements to be certified. The questionnaire includes both opened and closed questions. Correlative items (questions) are also added in order to help the respondent for clear and precise answers.

B. Data analysis and research findings

The questionnaire had an adequate pattern, starting with questions for respondents′ demographic characteristics and finishing with questions about the

Information Security Management System certification. The questionnaire was distributed to more than 300 respondents, only 174 have filled it.

Overall, the structure of the sample in terms of gender was rather balanced (110 - 63% men and 64 - 37% women). Respondents' age (see Figure 2) was mostly of 20-25 years (70%); 18% were of 26 - 30 years; only 13% were older than 30 years.

Respondents' age	**No. of respondents**	**% of respondents**
20-25	121	70%
26 - 30	31	18%
31 - 35	8	~5%
36 - 40	1	~1%
41 - 45	4	2%
>46	9	5%

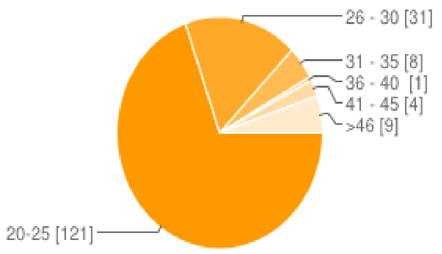


Fig. 2. The repartition of the respondents' age

Regarding the respondents' university degree, most of them have a technical degree (computer science), but there were respondents with a non technical degree: higher education in the field of economics, law, public order and national security, etc. Regarding the organizations' activity domains which the respondents work in, the repartition is shown in the Figure 3 and includes: IT, education and research, national security, telecommunications, public administration, commerce, e-business, financial services, consultancy, civil engineering.

Organizations' activity domains	No. of respondents	% of respondents
IT	100	58%
Education /Training / Research	20	11%
National security	14	8%
Telecommunications	7	4%
Commerce	6	3%
Other	27	16%

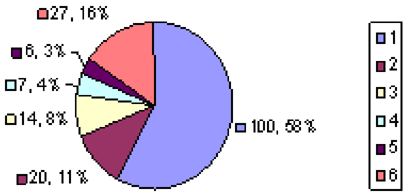


Fig. 3. The repartition of the organizations' activity domains which the respondents work in

The surveyed organizations have more than 250 employees (50%), 32% less than 50 employees, 7% have between 51 and 100 employees and 11% have between 101 and 250 employees (see Figure 4). 44% of the respondents have a middle and operational management position, 5% have a top management position, and 51% are in executive level positions.

Number of employees	No. of respondents	% of respondents
≤ 50	55	32%
51 - 100	13	7%
101 - 250	19	11%
> 250	87	50%

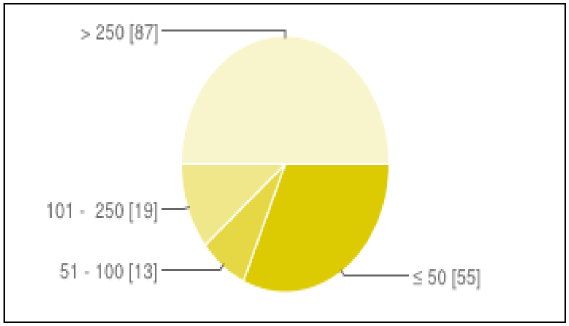


Fig. 4. The number of employees in the surveyed organizations

Regarding the type of the surveyed organizations, in the Figure 5 the repartition is shown: 35% are public, 58% are private and 7% are mixed organizations.

Type of the organization	No. of respondents	% of respondents
Public organization	61	35%
Private organization	101	58%
Mixed organization	12	7%

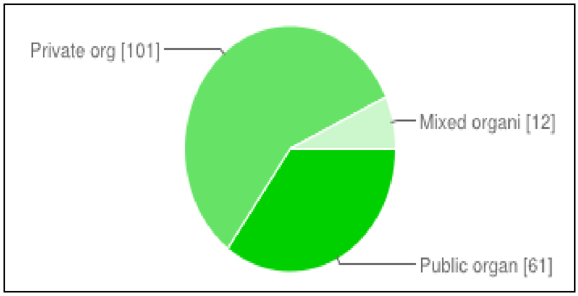


Fig. 5. The type of the surveyed organizations

According to the study, 33% of the organizations have no ISO certification, only 25% of them have an Information Security Management System certified, other management system certifications are as follows (see Figure 6): Integrated Management System (ISO 27001 + 9001 or other combination) – 12%, Quality Management System (ISO 9001:2008) – 20%, other or no answer – 10%.

The data analysis regarding the certification (and its benefits) of an Information Security Management System according to ISO 27001:2005 or ISO 27001:2013 reveals some interesting research findings. 79% of the respondents believe that an ISO 27001 certification would have benefits for their organizations (see Figure 8). Also, 80% of them think that an ISO certification (not only an ISMS certification) would also have benefits for their companies (see Figure 7).

Type of certification	No. of respondents	% of respondents
ISMS (ISO 27001:2005 or 27001:2013)	44	25%
Quality Management System	34	20%
Integrated Management System	21	12%
NO certification	58	33%
Other or no answer	17	10%

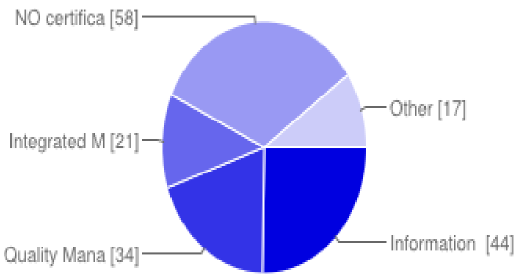


Fig. 6. The type of the certification in the surveyed organizations

ISO certification would have benefits for organization	No. of respondents	% of respondents
YES	140	80%
NO	34	20%

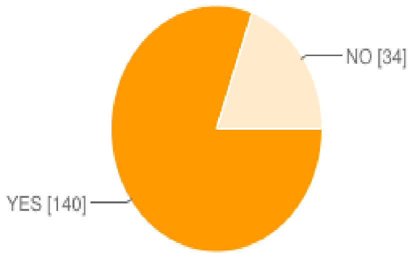


Fig. 7. The repartition of the respondents answers regarding the benefits of an ISO certification

ISMS certification would have benefits for organization	No. of respondents	% of respondents
YES	139	79%
NO	35	21%

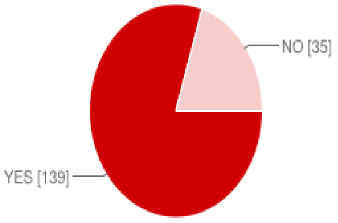


Fig. 8. The respondents answers regarding the benefits of an ISMS certification

Only 34% of the organizations in the research have the intention to certify or recertify a management system, 24% intend to certify or recertify an Information Security Management System according to ISO 27001 international standard. There is a big percentage of the respondents (66%) with the answer NO / I DO NOT KNOW. This is an interesting result because the organizations are aware of the certification benefits (see Figures 7 and 8), but the percentage is not the same (is smaller) regarding the intention of certification or recertification – some possible causes of such a situation would be the costs of certification or the priorities of the top management. The result is not equally interesting (the percentages are almost the same) if the comparison is made between the Figure 6 (the type of the certification in the organizations) and the Figure 9 (the intention of an organization to be certified / recertified).

The intention of an organization to be certified / recertified	No. of respondents	% of respondents
YES, ISO 27001	41	24%
YES, Other ISO	18	10%
NO / I DO NOT KNOW	115	66%

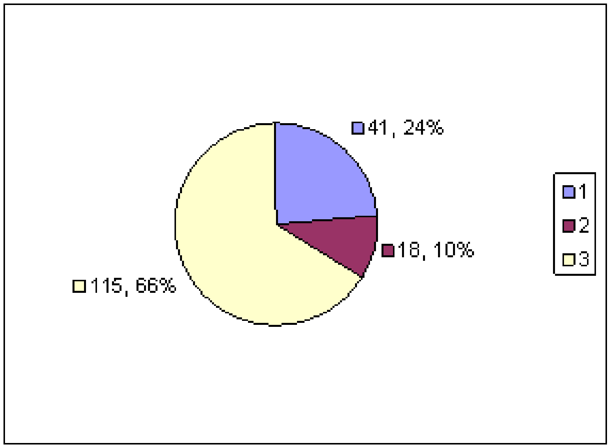


Fig. 9. The intention of an organization to be certified / recertified

As the data analysis reveals, 51% of the Romanian surveyed organizations know the requirements and / or procedure for the implementation / ISO certification of a management system. At the question:

Does your organization know the requirements / procedure for the implementation / ISO certification of a management system (in particular Information Security Management System according with ISO 27001)?

the respondents answers are presented in the Fig. 10.

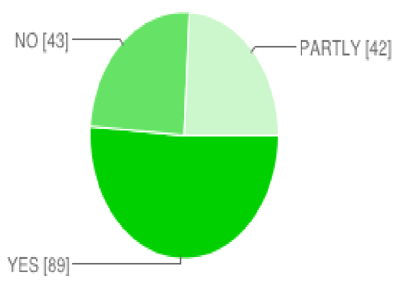
The organization knows the requirements/ procedure	**No. of respondents**	**% of respondents**	
YES	89	51%	
NO	43	25%	
PARTLY	42	24%	

Fig. 10. The respondents answers regarding the level of knowledge of the requirements / procedure for the implementation / ISO certification of a management system (in particular Information Security Management System according with ISO 27001)

3. Final aspects

Nowadays, the mankind is in front of a global and dynamic society where the information (security) represents power. It very important to have the right tools to protect sensible information of state or organizations. The cyber attacks, the threats on the organizational information and other security problems can be kept under control only by a close cooperation on two components:

- ➢ the knowledge component;
- ➢ the prevention component;

between the state and the business and academic community, professional associations and non-governmental organizations.

This paper tries to outline the importance of the information security assurance and of the implementation and certification of an Information Security Management System in companies. This certification provides benefits for organization and reliance for customers.

Even though this research has several shortcomings such as sample selection or number of respondents, there are several conclusions:

- There is still a big percentage of organizations that have NO certification - 33%; this is a real problem in Romanian companies because information security must be assured in order to create a framework to achieve organizational objectives and a way to do this is to have in company an ISO 27001 certification;
- Another important conclusion is related to the percentage (more than 50%) of the organizations that have no intention (or don’t know) to be certified or recertified;
- A positive aspect is that 80 % of the respondents believe that an ISO (not only 27001) certification would have benefits for their organizations.

Acknowledgement

The work has been funded by the Sectoral Operational Programme Human Resources Development 2007-2013 of the Ministry of European Funds through the Financial Agreement POSDRU/159/1.5/S/132395.

REFERENCES

[1]. *I. Chifu*, The liberal approach towards energy security through interdependence at risk, U.P.B. Scientific Bulletin, Series D, vol. 76, Iss. 4, ISSN 1454-2358, 2014.

[2]. *K. Naresh, D. Birks,* Marketing Research. An Applied Approach, Third European Edition, Prentice Hall, London, 2007.

[3]. *D. Pipkin*, Information security: Protecting the global enterprise. New York: Hewlett-Packard Company, 2000.

[4]. *A. A. Purcărea, B. Ţigănoaia*, "Considerations on information security in Romania", The Journal of the Romanian Managers and Economical Engineers Association - Review of Management and Economic Engineering, Vol. 9, Nr. 1, ISSN 1583-624X, 2010.

[5] *B. Ţigănoaia, F. Iacob*, "Low distortion and robust steganography on parallel architecture Cell BE using a shared color palette and a shared hash", U.P.B. Scientific Bulletin, Series C, Vol. 72, Iss. 3, ISSN 1454-234x, 2010.

[6]. *** ISO 27k family of standards, http://www.iso.org/iso/, accessed in 2014.

[7].***An Introduction to Information, Network and Internet Security, http://security.practitioner.com/introduction/infosec_8_6.htm., accessed in 2015.