THE CERTIFICATION OF ANINFORMATION SECURITY MANAGEMENT SYSTEM –RESEARCH IN THE BULGARIAN ORGANIZATIONS

Bogdan Ţigănoaia, Assist. Prof., PhD, Eng., PolitehnicaUniversity of Bucharest

Abstract:This paper presents aspects regarding the Information Security Management Systems in organizations. There are highlighted, among other, some of the international ISO standards in the field of security and the benefits of an ISO 27001:2013 certification. A research based on a questionnaire regarding this issue was made, the target group of the research were the Bulgarian organizations. The data are analyzed and the findings of this study are highlighted. Final aspects based on the research results are also presented.

Keywords:*information security, standards, organization, management system, research*

1. Introduction and theoretical context

An information security management system (ISMS) provides controls to protect organizations their most fundamental asset, information [1]. Due to the advance of mobile network, E-commerce, Open Networks, and Internet Banking, Information Security Management System (ISMS) is used to manage information of their customer and themselves by a government or a business organization [2].

ISO 27001 is the international standard that helps organizations keep information assets secure. Security 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), and terms and definitions commonly used in the ISMS family of standards [5].
- ✓ *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 [5].
- ✓ *I.S.O. / I.E.C. 27002:2013 - Information technology – Security techniques – Code of practice for information security controls* – ISO/IEC 27002:2013 gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s).It is designed to be used by organizations that intend to:
  - o select controls within the process of implementing an Information Security Management System based on ISO/IEC 27001;

- o implement commonly accepted information security controls;
- o develop their own information security management guidelines [5].

✓ *Other standards:*

- □ *I.S.O./I.E.C. 27003:2010* - Information technology -- Security techniques -- Information security management system implementation guidance;
- □ *ISO/IEC 27014:2013* - Information technology -- Security techniques -- Governance of information security.
- □ *I.S.O./I.E.C. 27035:2011*– Information technology -- Security techniques -- Information security incident management;

✓ *Other standards under development:*

- o *I.S.O./I.E.C. 27033–6*– Information technology -- Security techniques -- Network security -- Part 6: Securing wireless IP network access;

An accredited certificate from a certification body will help an organization to manage the security of assets such as financial information, intellectual property, etc. ISO27001 is a widely adopted ISMS standard that sets specific information security requirements for the management system. Organizations that claim to have adopted ISO27001 can be formally audited and certified to comply with the ISO27001 standard [1].

With ISO 27001:2013 an organization can demonstrate to existing and potential customers, suppliers and shareholders the integrity of its data and systems and its commitment to information security [7].

One of the most important benefits of such a certification is related to the customers: the implementation of an ISMS (that implies the implementation of effective information security processes) is a powerful tool to win the customers' confidence and helps the organization to create a trusting relationship with them. The main benefits of ISO 27001 certification are summarized below [6]:

- Manage and minimize risk exposure and allow for secure exchange of information;
- Keep confidential information secure and build a culture of security;
- Protect the company, assets, shareholders and directors;
- Deliver consistent services or products;
- Provide customers and stakeholders with confidence in how the organization manages risk;
- Maintain compliance with legislative and regulatory requirements;
- Enhance customer satisfaction, resulting in improved client retention.

2. Research in the Bulgarian organizations

A. Research methodology

In this part of the paper, based on a productive cooperation with Prof. Stanimir Stanev from Shumen University, Bulgaria, a pilot study has been conducted, having as target group the organizations from Bulgaria. The focus point of the research was related to the implementation and certification of an Information Security Management System according to ISO 27001:2013 international standard in Bulgarian organizations. The main objectives of the research were:

- To study aspects (the benefits, the intention of certification, procedure, requirements etc) regarding the implementation and certification of a management system, in particular of an Information Security Management System in Bulgarian organizations;
- To develop some conclusions, based on the research findings on a topic that is very actual and important for Bulgarian companies: information security assurance and certification of an Information Security Management System in Bulgarian organizations.

Variables Measurement

There are two types of variables: nominal scaled and variables regarding the certification of an Information Security Management System. The structure of the relevant variables of the research, as a summary, is presented in the Table 1.

Table 1. The map of research variables

Research variables		**Conceptual description**
Nominally Scaled Variables	Demographic Variables	Gender, age, education, professional background – position in the organization etc
		Organizational characteristics: type, number of employees, fields of activity etc
Variables regarding the certification of an Information Security Management System in Bulgarian organizations		Type, benefits etc of certification
		Intention, requirements and procedure to be certified

The research is based on a questionnaire that includes both opened and closed questions. Correlative items (questions) are also added in order to help the respondent for clear and precise answers. The qualitative questions are measured using a three point scale (e.g. YES, NO, PARTLY) (adaptation from [3]). The questionnaire, starting with questions for respondents′ demographic characteristics and finishing with questions about the certification of an Information Security Management System in Bulgarian organizations, contains issues regarding (selection): organizational characteristics of the Bulgarian companies: type, number of employees, fields of activity etc; type, benefits etc of certification; intention, requirements and procedure to be certified etc. The questionnaire was distributed to more than 100 respondents / organizations from Bulgaria. The number of daily responses is shown in the Figure 1.

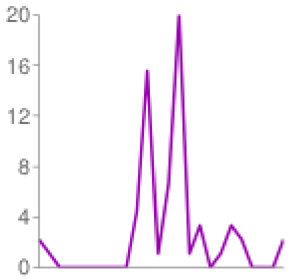


Figure 1: The number of daily responses – research in the Bulgarian organizations

B. Data analysis and research findings

Overall, the structure of the sample in terms of gender was not balanced (according to Figure 2, 78% men and 22% women).

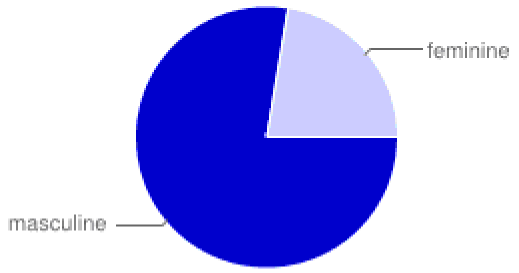
<table>
<tr><th>Gender</th><th>% of respondents</th><td rowspan="3"> </td></tr>
<tr><td>masculine</td><td>78%</td></tr>
<tr><td>feminine</td><td>22%</td></tr>
</table>

Figure 2: The repartition of the respondents in terms of gender

Respondents' age (see Figure 3) was mostly of 36-40 years (33%); 26% were of 31 - 35 years; 14% were of 41-45, 12% were of 26-30, only 9% were older than 46 years.

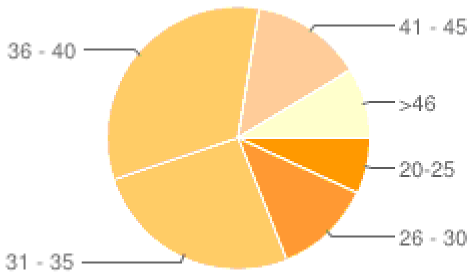
<table>
<tr><th>Respondents' age</th><th>% of respondents</th><td rowspan="7"> </td></tr>
<tr><td>20-25</td><td>6%</td></tr>
<tr><td>26 - 30</td><td>12%</td></tr>
<tr><td>31 - 35</td><td>26%</td></tr>
<tr><td>36 - 40</td><td>33%</td></tr>
<tr><td>41 - 45</td><td>14%</td></tr>
<tr><td>>46</td><td>9%</td></tr>
</table>

Figure 3: The repartition of the respondents' age

Most of the respondents have their higher education in the fields of informatics, computer science and economics, but there were respondents with university degree in other fields such as: mechanical and electrical engineering, electronics, veterinary medicine etc. Bulgarian organizations, part of the research, are active in the following spheres of activity: IT, education and research, commerce, financial services, consultancy, national security, telecommunications, public administration, e-business, civil engineering (the repartition can be viewed in the Table 2).

Table 2. The spheres of activity in Bulgarian organizations which were part of the research

Bulgarian organizations active in	**%**
IT	40%
Education / Training / Research	21%
Commerce	9%
Financial services	7%
Consultancy	5%
National security	3%
Other	15%

10% of the respondents have a top management / strategic level managerial position in the organization, 47% operational and middle level management positions, and 43% have no managerial functions (they are in an executive level position in a Bulgarian organization – see Figure 4).

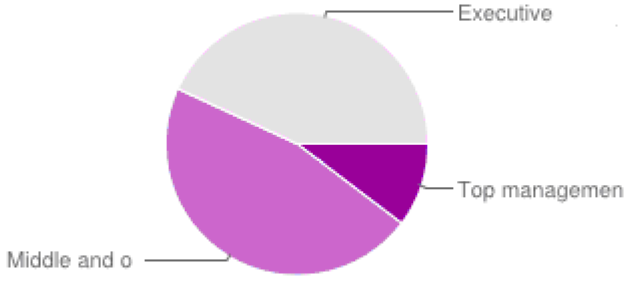
Respondents position in a Bulgarian organization	**% of respondents**	
Top management level	10%	
Middle and operational management level	47%	
Executive level	43%	

Figure 4: The repartition of the respondents' position in a Bulgarian organization

The Bulgarian organizations in the study have less than 50 employees (57%), only 16% have more than 250 employees, 17% have between 101 and 250 employees and 10% have between 51 and 100 employees (see Figure 5).

Number of employees	%
≤ 50	57%
51 - 100	10%
101 - 250	17%
> 250	16%

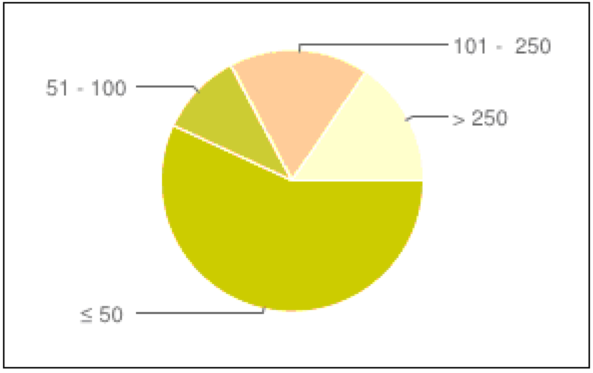
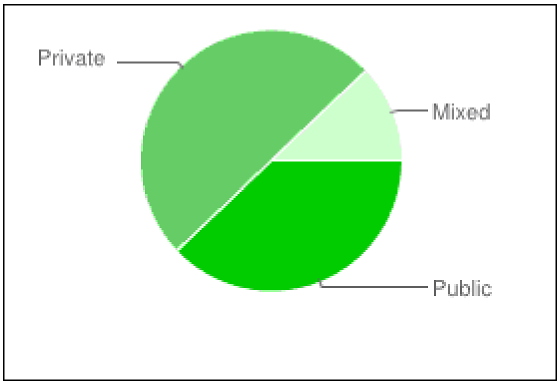


Figure 5: The number of employees in Bulgarian organizations which were part of the study

Regarding the type of the Bulgarian organizations part of the research, the Figure 6 presents the repartition: 38% are public, 50% are private and 12% are mixed organizations.

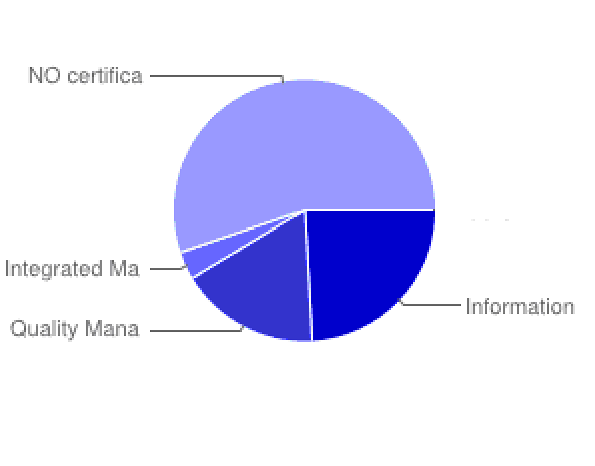
Type of the organization	%
Public organization	38%
Private organization	50%
Mixed organization	12%



▪ Figure 6: The type of the Bulgarian organizations which were part of the study

Data analysis results show that 55% of the Bulgarian organizations, part of the research, have no certification (see Figure 7). On the other hand, 25% of Bulgarian companies have an Information Security Management System (ISO 27001:2005 or 27001:2013) and 17% a Quality Management System (ISO 9001:2008) certification. Only 3% have an Integrated Management System (ISO 27001+ 9001 or other combination).

The type of the certification	%
ISMS (ISO 27001:2005 or 27001:2013)	25%
QMS(ISO 9001:2008)	17%
IMS (ISO 27001+ 9001 or others)	3%
NO certification	55%

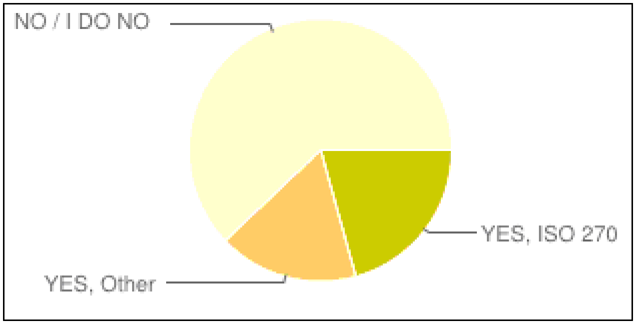


▪

Figure 7: The type of the certification in the Bulgarian organizations, part of the research

▪

Another important finding is related to the intention of the Bulgarian organizations to be (re)certified (see Figure 8). A big percentage, 62% of the organizations have no intention to be (re)certified according to an ISO international standard. 21% have the intention to make an Information Security Management System certification or recertification, 17% other ISO standards (re)certification.

The intention to be (re)certified	**%**	
Yes, ISO 27001	21%	
Yes, other ISO	17%	
No / I do not know	62%	

▪

Figure 8: The intention to be (re)certified in the Bulgarian organizations, part of the research

Other important findings:

1. 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 data analysis reveals the results presented in the Figure 9:

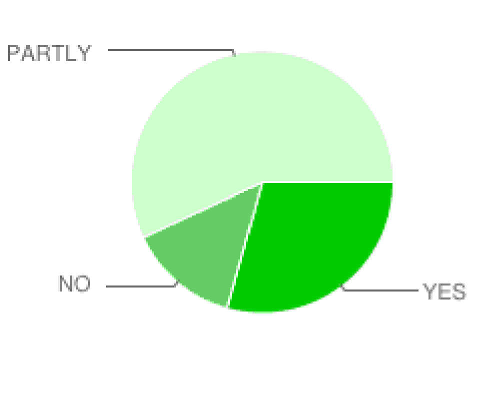
The Bulgarian organizations know the requirements/ procedure	**%**	
Yes	29%	
No	14%	
Partly	57%	

Figure 9: The repartion regarding the level of knowledge of the requirements / procedure for the implementation / ISO certification of a management system in Bulgarian organizations

▪ 2. At the question: *Do you think that an ISO certification would have benefits for your organization?,*

the findings are shown in the Figure 10:

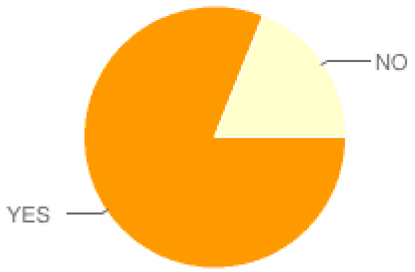
Do you think that an ISO certification would have benefits for your organization?	**%**	
Yes	81%	
No	19%	

Figure 10: The repartition regarding benefits of an ISO certification in Bulgarian organizations

- 3. At the question: Do *you think that an ISO 27001 (Information Security Management System) certification would have benefits for your organization?*,

the analysis can be viewed in the Figure 11:

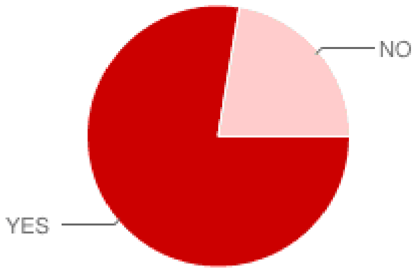
Do you think that an ISMS certification would have benefits for your organization?	**%**	
Yes	78%	
No	22%	

Figure 11: The repartition regarding benefits of an ISMS certification in Bulgarian organizations

It is interesting to make a correlation (and some comments) between the results in the Figures 7, 8 and 9 and the findings from Figures 10 and 11. Most of the Bulgarian organizations have no certification, are undecided regarding the intention to be (re)certified, but what is important for future is that big percentages of them know partly the requirements / procedure for the implementation / ISO certification of a management system and the Bulgarian companies think that an ISO or particularly an ISMS certification would have benefits in achieving the organizational objectives.

3. Final aspects

According to [4], the old wisdom of management gain more importance in information security management. This paper tries to outline the importance of Information Security Management System certification in companies as an important pylon in achieving information security. The ISO 27001:2013 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:

- From the data analysis, 55% of the Bulgarian organizations, part of the study, have no certification. On the other hand, only 25% (it is a very small percentage) of the Bulgarian companies have an Information Security Management System (ISO 27001:2005 or 27001:2013).
- Another important conclusion is related to the intention of the Bulgarian organizations to be (re)certified. A big percentage, 62% of the organizations have no intention (or don't know) to be (re)certified according to an ISO international standard.
- A positive aspect is that 78 % of the respondents believe that an ISO 27001 certification would have benefits for their organizations.

Acknowledgements

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. I would like to thank Prof. Stanimir Stanev for gathering data and its support in this research.

References

[1] Nykänen, R., Hakuli, M., *Information security management system standards: A gap analysis of the risk management in ISO 27001 and KATAKRI*, 12th European Conference on Information Warfare and Security 2013, ECIW 2013, pags 344-350, Jyvaskyla, Finland, 11 July 2013 through 12 July 2013.

[2] Jo, H., Kim, S., Won, D., *A study on comparative analysis of the information security management systems*, 2010 International Conference on Computational Science and Its Applications, ICCSA 2010; Volume 6019 LNCS, Issue PART 4, Pages 510-519, Fukuoka; Japan; 23 March 2010 through 26 March 2010.

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

[4] Humpert-Vrielink, F. , Vrielink, N., *A modern approach on information security measurement*, 14th Information Security Solutions Europe Conference, ISSE 2012; Brussels; Belgium; 23 October 2012 through 24 October 2012; Code 98644, 2012.

[5] ISO 27k family of standards (http://www.iso.org/iso/), accessed in 2014.

[6] http://www.cert-int.com/services/iso-27001-information-security/, accessed in April 2015.

[7]http://www.sgs.bg/en/Health-Safety/Quality-Health-Safety-and-Environment/Risk-Assessment-and-Management/Security-Management/ISO-27001-2013-Information-Security-Management-Systems.aspx , accessed in April 2015.