A PRELIMINARY MODEL TO ASSESS THE COMPANY' S READINESS FOR AN ISO / IEC 27001:2013 INFORMATION SECURITY MANAGEMENT SYSTEM

Bogdan Ţigănoaia, Assist. Prof., PhD, "Politehnica" University of Bucharest

Abstract: An Information Security Management System is one of the modern solutions in order to assure information security in an organization. Through an ISMS, the necessary framework for achieving the organizational objectives and efficiency and efficacy is assured. The paper presents some aspects regarding the news / changes in ISO / IEC 27001:2013 international standard, an analysis regarding the correlation between business needs and features and benefits of the ISO 27001:2013 standard. There is also proposed a model to assess the organization's readiness for an ISO / IEC 27001:2013 Information Security Management System. It is a self-assessment of the organization through the proposed model which allows to identify where is the organization in the ISO / IEC 27001 process. The self-assessment can be also considered for an organization a starting point in a further decision regarding the implementation in the company (quickly or not, depending on the level of readiness) of an ISMS according to new international standard, ISO 27001:2013.

Keywords: information security, management systems, self-assessment, organization's readiness, ISO standards.

1. Introduction

Information security in an organization is very important in achieving protection, predictability and finally profit. According to B.S.I. Group (British Standards Institution), successful businesses understand the value of *accurate information* and *secrecy*. One modern solution (with a lot of advantages – see chapter 2) to achieve security for organizational information is through an *ISMS - Information Security Management System,* according to the international standard ISO/IEC 27001:2013. A first step in a further decision regarding the adoption of an ISMS according to ISO / IEC 27001:2013 is a self-assessment, through a (preliminary) model, in order to establish the level of company's readiness for an ISO 27001:2013 Information Security Management System.

An organization can be in one of the following situations:

- ✓ in the organization **is implemented and certified an ISMS** according to ISO 27001:2005 and the company is interested to make the self-assessment (use the model) in order to see where is in the ISO 27001 process (related to the requirements of ISO 27001:2013). Based on a guide for transition from ISO 27001:2005 to ISO 27001:2013, the organization can achieve (quickly or not, depending on the level of readiness) the requirements of the new standard;

- ✓ in the organization **is not implemented an ISMS** and the company is interested to make the self-assessment (use the model) in order to see where is in the ISO 27001 process (related to the requirements of ISO 27001:2013). If the organization has a high level of readiness, it is an easier and quicker process of implementation and certification. If not, the organization must have attention regarding the requirements and more work is necessarily in order to implement and certify an ISMS.

2. News in ISO 27001:2013. The correlation between the business needs and features& benefits of the standard

The previous version (2005) of the ISO 27001 was replaced by a new version in 2013.

There are a lot of changes in the newer version of the standard, some of them are presented below:

- **changes to the structure of the standard -** the new structure of the standard is aligned with Annex SL to Part 1 of the ISO/IEC Directives. It is intended that all management system standards will adopt this format at their next revision. This will introduce further consistency for organizations that have integrated management systems that cover multiple standards, such as ISO 9001, Quality Management Systems and ISO 14001, Environmental Management Systems [1]. The new structure of the ISO/IEC 27001:2013 is:
  - ✓ ***0. Introduction***
  - ✓ ***1. Scope***
  - ✓ ***2. Normative references***
  - ✓ ***3. Terms and definitions***
  - ✓ ***4. Context of the organization***
  - ✓ ***5. Leadership***
  - ✓ ***6. Planning***
  - ✓ ***7. Support***
  - ✓ ***8. Operation***
  - ✓ ***9. Performance evaluation***
  - ✓ ***10. Improvement***
- **some new requirements were introduced** (selection - the number of chapter in the standard):
  - ✓ 4.2(a); 4.3(c);
  - ✓ 5.1(b);
  - ✓ 6.1.1(a); 6.2(b);
  - ✓ 7.3(a); 7.4(a);
  - ✓ 8.1;
  - ✓ 9.1(c); 9.1(d); 9.1(f);
  - ✓ 10.1(a); 10.1(a)(1); 10.1(a)(2); 10.1(e); 10.1(f).
- **some requirements were eliminated (selection):**

- ✓ 4.3.3 the controls needed for the identification, storage, protection, retrieval, retention time and disposition of records shall be documented and implemented [2].
- ✓ 8.3(e) the revision of the taken preventive actions;
- ✓ 8.2, 8.3 the documented procedure for corrective and preventive actions must define requirements in this direction;

- **requirements for documented information** – in ISO 27001:2013 there are requirements for *documented information*, not for *documented procedures and records*, as in ISO 27001:2005. According to the new version of the standard [3], the following documented information are mandatory for certification:
  - ✓ ISMS scope (4.3)
  - ✓ Information security policy (5.2)
  - ✓ Information security risk assessment process (6.1.2)
  - ✓ Information security risk treatment process (6.1.3)
  - ✓ Statement of Applicability (6.1.3 d))
  - ✓ Information security objectives (6.2)
  - ✓ Evidence of the competence of the people (7.2)
  - ✓ Documentation information determined as being necessarily for effectiveness (7.5.1b)
  - ✓ Operational planning and control information (8.1)
  - ✓ The results of the information security risk assessments (8.2)
  - ✓ The results of information security risk treatment (8.3)
  - ✓ Evidence of the monitoring and measurement results (9.1)
  - ✓ Evidence of the audit program(s) and the audit results (9.2)
  - ✓ Evidence of the results of management reviews of the ISMS (9.3)
  - ✓ Evidence of the nature of nonconformities identified and any subsequent actions taken and corrective actions (10.1)

In the next section, an analysis (based on [4]) regarding *the correlation between the business needs and features and benefits of the ISO 27001 standard is presented.*

Table 1. The correlation between business needs, features of the standard and benefits

Business need	**Feature of the standard**	**Benefits (what is useful for the business in the standard)**
To reduce risk of incidents and to assure information security	Procedure for the identification of relevant risks, understanding of how the risk is formed and evaluation of improvements.	✓ Fewer incidents. ✓ Fewer disruptions. ✓ Less time spent on responding to accidents and incidents. ✓ More time to spend on proactive measures. ✓ Lower client audit requirements.
To attract more clients and investors.	Operational controls to be in place.	✓ Less resource spent on finding new customers and investors.

1. To protect and enhance reputation. 2. Confidence in organization to all interested parties 3. Market assurance (an ISMS is a powerful marketing instrument)	Operational controls to be in place	✓ Less negative press meaning less time and money spent on damage limitation measures. ✓ Better able to reassure customers, internal and external interested parties. ✓ Opportunities for positive PR.
Informed business decision making.	1. Roles and responsibilities to be defined. 2. Staff to be trained and competent. 3. Worker communication, participation and consultation in the ISMS required.	✓ Greater productivity. ✓ Less time and money spent on responding to incidents.
To control information but not unduly affect business processes.	1. Operating controls to be in place. 2. Procedures for overview and testing to be in place.	✓ Understanding of business information processes. ✓ Better able to reassure customers and internal parties.

3. A model to assess the organization's readiness for an ISO / IEC 27001:2013 Information Security Management System

According to A. A. Purcarea (2003) [6], a model is the representation of a system which indicates an image of reality (a system of objects, phenomenon, concepts). The models can be classified in (selection, function of the science which they operate in) [7]:

- ✓ Economical models;
- ✓ Sociological models
- ✓ Biological models
- ✓ Organizational models etc.

In another classification, function of the tool used for their description, the models can be [7]:

- ✓ Graphical models;
- ✓ Analogical models;
- ✓ Mathematical models;
- ✓ Physical models;
- ✓ Reference models etc.

The steps for elaboration of a model are [6]:

- ✓ *The wording of the model* – the first step has a preparatory target, the system studied must be well-known; the wording of the problem, what the model is prepared for, implies the existence of clear and valuable information;
- ✓ *The elaboration of the model* – the second step consists of the application of some tools used for pattern making; the correlation between the results and the tools used must be done;
- ✓ *The validation of the model* – the implementation of the model in a real system and then the improvement of the model or simplification of it (if it is possible). The quality of the model can be evaluated by comparison between the working of the model and the system.

The implementation and certification of an Information Security Management System in an organization according to ISO 27001 provides confidence to all interested parties (stakeholders) – clients, business partners etc. The assessment, through a model, of the company's readiness for an ISO/IEC 27001 Information Security Management System is an important step done before the implementation and certification of an ISMS. This paper proposes such a model that is based on the ISO 27001:2013 (and other standards from ISO 27000 family) international standard and tries to bring together, through an original thinking, aspects and requirements presented in international standards in the field of information security. The proposed model is especially suitable for organizations (all types and dimensions) that already have implemented (and certified) an ISMS according to ISO 27001:2005 and want to achieve the new requirements of the ISO 27001:2013, or have the intention to implement and certify an ISMS according to ISO 27001:2013. The model is not an exhaustive one, it is very difficult to do that. All organizations are different and this model needs to be interpreted in the context of the individual needs of each organization. The organization is helped to make a self-assessment / analysis of its readiness for an ISO/IEC 27001 Information Security Management System.

The model was designed related to the new structure of the ISO 27001:2013 and some aspects are based on [5]. It has the following elements / modules that are presented in the Figure 1. and detailed below:

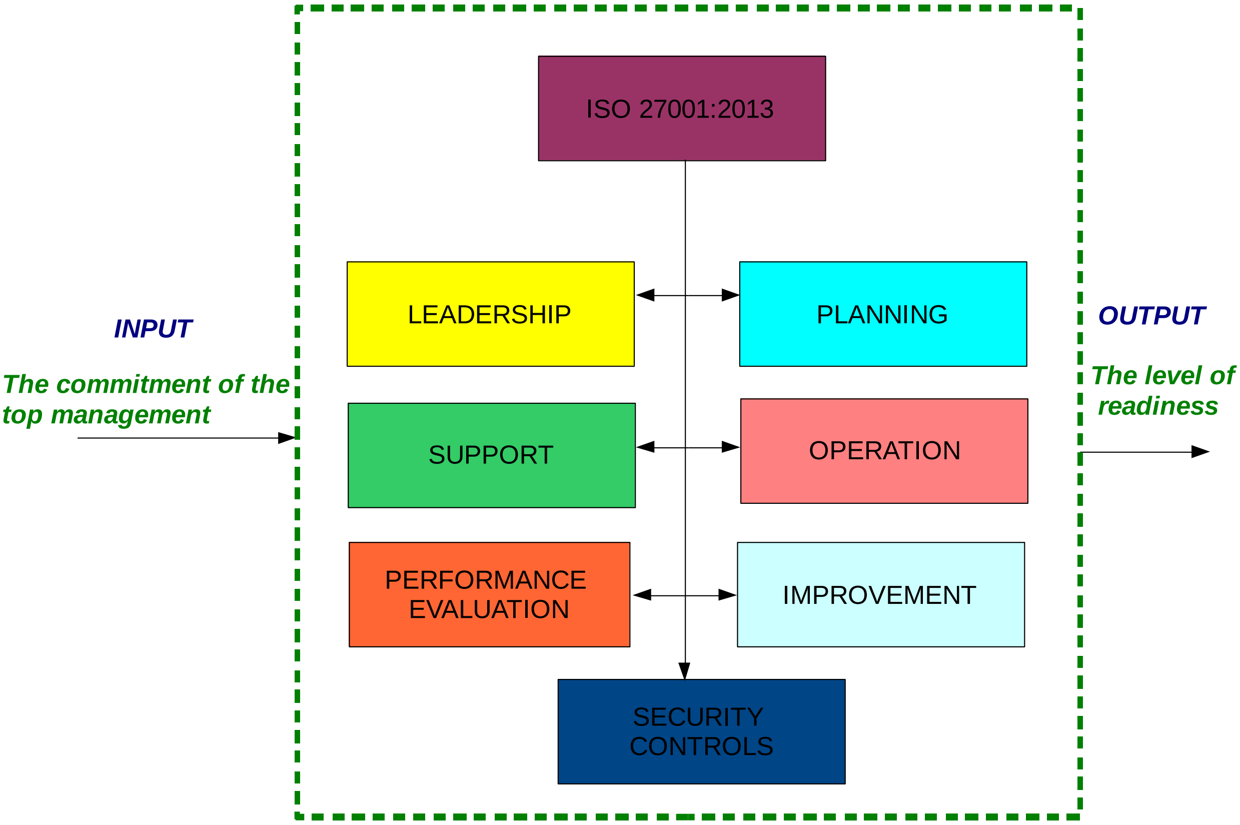

Figure 1.The preliminary model to assess the company's readiness for an ISO/IEC 27001 ISMS

- **LEADERSHIP – 19 points:**

  ✓ Does the management of the organization provide commitment to the ISMS (example: establishing the information security policy and objectives and communicating the importance of meeting these objectives to the organization) ? – *5 points*

  ✓ Are the required resources to establish, implement, operate, monitor, review and improve the ISMS determined and provided? - *5 points*

  ✓ Are responsibilities regarding information security assurance in organization defined? – *4 points*

  ✓ Are there periodical courses for employees responsible for information security assurance in organization? –*3 points*

  ✓ Do employees responsible for information security assurance have the required competence and training to perform their duties? – *2 points*

- **PLANNING – 18 points:**

  ✓ Is there an approved information security policy? - *3 points*

  ✓ Has the scope and boundaries of the Information Security Management System (ISMS) been defined? – *2 points*

- ✓ The management of risks is very important in organization - have the levels of risk been periodically estimated and determined as being within the acceptable level or requiring risk treatment (have options for risk treatment been identified and evaluated?) ? - 5 *points*
- ✓ Has the business impact for loss of confidentiality, integrity and availability, and the likelihood of security failures, been analysed and evaluated? – *3 points*
- ✓ Has a risk assessment method and the acceptable levels of risk been defined and documented? – *3 points*
- ✓ Is there a Statement of Applicability? A SA is showing which controls from ISO/IEC 27001 Annex A have been selected, the reasons for selection or non-selection, and the status of implementation - *2 points*

- **SUPPORT – 5 points:**

- ✓ Are the documented information - documents and records, related to the information security management system managed and controlled according to defined procedures? – *5 points*

- **OPERATION – 17 points:**

- ✓ Is there a risk treatment plan (actions, resources etc) for managing information security risks? – *4 points*
- ✓ Has the risk treatment plan been implemented? – *4 points*
- ✓ Is the operation of the ISMS (including the resources that are necessarily) being managed? – *4 points*
- ✓ Have controls (for detection and response to security incidents) been implemented? – *3 points*
- ✓ Has a training and awareness programme been implemented? – *2 points*

- **PERFORMANCE EVALUATION – 15 points:**

- ✓ The internal ISMS audits are conducted at planned intervals – *3 points*
- ✓ Are there monitoring and reviewing activities or processes to detect processing errors, attempted or successful security breaches, performance of people and/or technology, prevention of security events and to determine whether actions taken are effective? [5] – *3 points*
- ✓ Are regular reviews of effectiveness undertaken using the results of audits, incidents, measurements and feedback from interested parties? [5] – *3 points*
- ✓ Are risks (the acceptable level, residual risks etc) reviewed at planned intervals? – *3 points*
- ✓ Management reviews of the ISMS are made at planned intervals – *3 points*

- **IMPROVEMENT – 6 points:**

  - ✓ Are improvements identified, implemented and evaluated (in order to achieve the organizational objectives)? – *3 points*
  - ✓ Are appropriate corrective and preventive actions identified and implemented? – *3 points*

- **SECURITY CONTROLS – 20 points:** according to the author's experience and thinking a list of important security controls is proposed:

  - ✓ The organization has an access control policy (rules for audit logs of user activities, system events, access to operating systems, removable media, access to network, management of privileges and passwords, user registration procedure etc) based on business and security requirements – *3 points*
  - ✓ Are networks managed and controlled in order to protect from threats and maintain security for systems and application, and is there an agreement in place to maintain these security requirements? [5] – *3 points*
  - ✓ Do you take regular backups of information and software, and are backups tested regularly in accordance with an agreed backup policy? [5] – *3 points*
  - ✓ Information security risks from external parties are identified by the organization – *3 points*
  - ✓ The assets are inventoried (an asset has an owner and rules for use) - *2 points*
  - ✓ Do you perform background verification checks of all candidates for employment – in accordance with relevant regulations and in proportion to business requirements? [5] – *2 points*
  - ✓ There is in organization a physical security perimeter (for security sensitive areas etc) – *2 points*
  - ✓ Do you have confidentiality and / or non-disclosure agreements within your conditions of employment and contracts with suppliers? [5] – *2 points*

Regarding the level of readiness, some thresholds can be proposed as follows:

- ✓ 80-100 points: high level of readiness;
- ✓ 60-80 points: good level of readiness;
- ✓ 30-60 points: satisfactory level of readiness;
- ✓ <30 points: not satisfactory level of readiness.

4. Final aspects

The paper helps the organizations to discover news, features and benefits of the ISO 27001:2013 international standard related to the business needs. The proposed model is a tool that can be used by organizations to assess the company's readiness for an ISO 27001:2013 Information Security Management System. The model, by its output / results, helps an organization to identify where it is in the ISO 27001 process. The model / self-assessment can be also considered for organizations an important starting point in a further decision regarding the implementation and certification of an ISMS according to ISO 27001:2013 in the company.

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.

References

[1] SAI Global report – *New ISO/IEC 27001:2013 Information Security Management Systems*, http://www.saiglobal.com/, accessed in 2014.

[2] B.S.I. report: *Mapping between the requirements of ISO/IEC 27001:2005 and ISO/IEC 27001:2013*, 2014.

[3] ISO 27k family of standards (http://www.iso.org/iso/).

[4] BSI report: *ISO 27001 Information Security - Features and benefits*, accessed in 2014.

[5] B.S.I. document: *ISO/IEC 27001 Information Security Management System - Self-assessment questionnaire*, accessed in 2014.

[6] Purcărea A. A, *Management şi inginerie industrială. Modele matematice*, Ed. Niculescu, Bucuresti, p. 320, 2003.

[7] C. Fisher., *Researching and Writing a Dissertation*, 2nd edition, FT Prentice Hall, 2007.