Aspects regarding the implementation of information security standards in organizations

Mihai Bârsan
PhDc, *Transilvania* University of Brasov
E-mail mihai_c_barsan@yahoo.com

Information security is one of the major challenges of the information and knowledge based society. The preoccupation of organizations to ensure the security of information in the digital environment has led to the emergence of specific standards in the field. Thus, ISO 27000 brings together reference standards in the field. Starting from ISO 27001, which summarizes policies and procedures on physical, legal and technological security risks, this paper looks at the steps the organization must undertake to implement the standards.

Keywords: *ISO 27001; information security; databases; security policy*

1. Introduction

Information security has become an important concern in organizations that store information in digital archives.

In a study on Creating an Information Systems Security Culture through an Integrated Model of Employee Compliance (Ajaj et al 2014), and using a mixed-method approach, a group of managers shared knowledge of awareness, advocacy behaviors and challenges that influence their involvement in information security advocacy (Giraldo 2014).

The perception of human resources managers about the use of information security policy (Jobi 2012) shows that at that time there was much attitude towards the implementation of a security system within organizations.

ISO 27001 is an international standard published by the International Organization for Standardization (ISO), which describes the methodologies of information security management in an organization. The first review of the standard was published in 2005 and was developed on the basis of British Standard BS 7799-2. The latest revision of this standard was in 2013, resulting in ISO / IEC 27001: 2013.

The ISO 27001 standard can be implemented in any type of organization, whether public or private, irrespective of the field of activity, and is recommended for all entities managing a large amount of data stored in digital format.

By implementing ISO 27001, an independent certification body confirms that an organization complies with ISO 27001 information security procedures.

Organizations that choose to implement information security management standards need to go through a series of precursory steps and carry out a self-assessment of meeting minimum requirements.

The Information Security Management System (ISMS) should include specific interfaces for each internal department of the organization as well as for external users: beneficiaries, customers, partners, suppliers.

2. Methodology for implementation in organizations

2.1. Setting the Scope

The organization's internal structures involved in information management must carry out a risk assessment of all other internal departments to identify whether there is a risk to the information for which it is responsible.

In the assessment, the independent certification body must certify that the organization under review is able to handle the information safely, by checking the responsible department.

A first condition for implementing the standards is the clear delimitation of assets used by the department responsible for information security management: physical space used by department employees, local network, logistics facilities. For example, if the IT network used by the target department is also used by employees of other departments of the same organization (without segregation), there is no way to control only the flow of information within the domain.

Unfortunately, narrowing the scope of the ISMS Information Security Management System is sometimes impossible. Therefore, it is often necessary to extend the scope to the entire organization. This measure is especially recommended for small organizations operating in a single location.

In the case of large organizations, where the ISMS Information Management System at the level of the entire organization would generate huge costs, the scope will be limited to an independent organizational unit that interacts with the other departments exclusively on the basis of pre-established internal policies and procedures.

2.2 The ISMS policy

Another important step in the implementation of ISO 27001 standards is the drafting of an internal policy.

The ISMS policy is the most important document underlying the Information Security Management System. Like a Constitution, the document should include the basic information security aspects of the organization under review. Organization management must set a number of objectives in the field, as well as specific control mechanisms.

Numerous organizations chose to draft far too detailed policies, in the desire to regulate procedures specific to each possible situation, including in the ISMS Policy both the strategic objectives in the field of information security and the detailing of procedures applicable at the level of each department. Often, such overly detailed documents are not strictly enforced, as they cannot be fully understood by all responsible actors.

For this reason, ISO 27001, the main security standard for information, defines several levels of information security policies:

- High-level Policies (ISMS Policy) - are policies that define the organization's principles, goals and strategy;

- Detailed Policies - are policies that describe in detail an area of information security, regulating procedures, responsibilities and precise control mechanisms.

ISO 27001 sets out a number of minimum requirements regarding the content of the Information Security Management System (ISMS) policy:

- Setting goals;

- Analysis of the current context;

- Criteria for risk assessment.

The detailed policies, as mentioned above, are intended for operational use and should focus on a narrower range of specific activities. Such policies are:

- Classification policy;
- Policy regarding the use of information;
- Access control policy;
- Password policy;
- Network usage policy;
- Cryptographic control policy, etc.

ISO 27001 does not require the implementation of all these policies, the decision whether or not to act in a certain direction is taken following a process of risk assessment for the databases managed by the organization.

Detailed policies should regulate every aspect of the problem, so they have a much wider content.

Information security is a complex issue that cannot be defined by a single policy. Thus, ISMS will be a set of policies that will regulate access to information for each category of beneficiaries, aiming to cover all the risks identified by the evaluation process.

Any policy must be drafted with the sole purpose of reducing risks. The effectiveness of policies adopted by an organization can be seen over time, being proven by reducing the number of security incidents.

2.3. Risk Assessment Methodology

The security risk assessment is the most complex stage in the implementation of ISO 27001 standards. Based on the results of the evaluation, the main directions and the policies to be developed will be identified.

The main purpose is to identify the vulnerabilities, threats, risks and dangers to which an archive is exposed and to define acceptable risk levels.

If the evaluation process is not implemented correctly, there is a risk that the measures which will subsequently be taken, will not lead to the results assumed through the management system policy.

2.4 Risk Assessment and Treatment

At this stage, organizations that are in the process of implementing ISO 27001 standards will focus on correlating the identified risks with specific measures to reduce them. The measures must be applicable to the organization, taking into consideration the existing logistical facilities.

The purpose of the evaluation process is to outline a broad picture of the information security risks faced by the organization.

The purpose of the risk management process is to reduce or even eliminate risks that are not acceptable in relation to specific standards, by planning the use of the controls in Annex A.

In this context, a risk assessment report should be drawn up, including all the measures taken during the assessment and treatment processes.

2.5. Statement of applicability

Annex A of ISO 27001 includes a total of 114 controls on risk assessment and treatment. It is unlikely that an organization will have to apply all of these and for this reason it is necessary to determine those controls which are absolutely necessary in relation to the results of the evaluation.

An attempt to implement all controls could lead to bureaucratic procedures that are difficult to apply and will generate unnecessary costs within the organization.

At this stage, the Statement of Applicability (SoA) will be drawn up as a document listing all the controls and defining which are applicable and which are not, as well as the reasons for such a decision.

The document will also refer to the objectives to be achieved by using controls and will describe how to implement them.

The Statement of Applicability (SoA) is the document required to obtain the management authorization for the ISMS implementation.

2.6. Risk Treatment Plan

The risk treatment plan is an operative document, which defines how the SoA controls will be implemented, the responsible actors, the internal procedures, and the budget.

Basically, this document is the implementation plan of the Information Security Management System, and it is necessary in order to coordinate the whole process.

2.7. How to measure the effectiveness of controls

In order to measure the achievement of the objectives set for both the whole ISMS and for each applicable control, the organization will define specific modalities. These modalities must allow a clear measurement of the progress made at the organization level.

2.8 Implementation of mandatory procedures

At this stage, the four mandatory procedures and the applicable controls in Annex A will be implemented.

This process involves implementing a new behavior in the organization.

It is often necessary to apply new technologies or new policies and procedures that the responsible actors have to follow.

Most times people are reluctant to change, which is why the organization will pay special attention to the process of training and training.

2.9. Human resource training

Regardless of how effective the documented procedures are and how efficient the technology is, the most important factor in the implementation of the Information Security Management System remains the human resource.

Organization staff must be informed about new policies and procedures and must understand the need to apply them. At the same time, staff training activities involved in ISMS implementation must be organized.

2.10. ISMS Operation

Following the implementation of ISMS and human resources training, ISO 27001 becomes an ordinary routine in the organization.

The operation of the Information Security Management System requires recording (recordings) of the operating parameters, which have the role of contributing to the monitoring of compliance by the personnel and the external factors.

2.11. ISMS monitoring and internal audit

As part of the monitoring process, it will be checked whether the results achieve the objectives set. The incidents will be analyzed and it will be determined whether the procedures have been performed correctly.

Following the monitoring, corrective and / or preventive actions can be taken. If the existing or potential problems that may be harmful to the organization are not known, an internal audit must be carried out to find such things.

2.12. Management review

Management needs to know what is happening in ISMS, if the staff has performed its tasks, and if ISMS achieves the set goals. In this respect, management has to make essential decisions to correct deficiencies.

2.13. Corrective and preventive actions

The purpose of the ISMS management system is to ensure that all non-conformities are corrected, or even hindered. Thus, ISO 27001 requires that corrective and preventive actions will be carried out systematically, starting from the identification of the main cause of nonconformity, which will then be resolved and verified.

3. Final considerations and conclusions

The preoccupation of organizations to ensure the security of information in the digital environment has led to the improvement of specific standards and to the development of procedures designed to make the implementation of ISO 27001 easier.

The steps presented are the essential and binding steps to be followed for any organization, whether public or private, regardless of size or subject matter. Of course, in some cases, the procedure may be more complex, but this aspect depends on the specifics of the organization.

The correct and systematic implementation of the basic steps is essential to achieving the objectives of the Information Security Management System.

In practice, it was found that the absence of staff training, misconstruction of objectives and the choice of inadequate controls are the most common reasons for the failure of the ISO 27001 project.

References

Tapomoy, K., Shounak, G. and Shameek, G. (2015) Trends & Emerging Areas in Merchant Acquiring Industry, *International Journal of Economics and Finance*, 7(1), pp. 229-240, available: http://ccsenet.org/journal/index.php/ijef/article/view/41346/23870.

Giraldo, G. (2014). *Motivating Information Security Awareness (ISA): an Action Research Study*, dissertation, Syracuse University.

Jobi, O. (2012). *Human Resources Managers' Perception of Utilization and Adoption of Information Security Policy*, dissertation, Capella University.

(ISO 27001): *Information Security Management System* (2013), Geneva: International Organization for Standardization.

(ISO 27001): *Information Security Management System - Annex A* (2013), Geneva: International Organization for Standardization