Some Aspects Regarding the Information Security Management System within Organizations – Adopting the ISO/IEC 27001:2013 Standard

Bogdan ȚIGĂNOAIA

Politehnica University of Bucharest,
313, Splaiul Independentei, Bucharest, Romania
bogdantiganoaia@gmail.com

Abstract: Information security in an organization is one of the most important pillars in achieving organizational objectives. It does not produce profit but it offers the necessary framework for efficiency and efficacy in organization. Information security can be provided in an organization through the implementation and certification of an ISMS–Information Security Management System. This paper presents some aspects regarding the information security management system in an organization and underlines the importance of the adoption of an ISMS and the new elements in ISO/IEC 27001:2013 (new concepts, requirements and changes introduced in the standard). An analysis regarding the correlation between the business risks and features & advantages of the ISO/IEC 27001 standard is presented. There is also proposed a guide for adopting the ISO/IEC 27001:2013 standard, which implies a self-assessment of the organization (which allows to identify where the organization in the ISO/IEC 27001 process is) and strategies (concrete steps and the allocation of resources). The proposed guide will help the organization to understand the relationship between ISO/IEC 27001:2013 and its predecessor ISO/IEC 27001:2005.

Keywords: information security, standards, management systems, organizations, ISO/IEC.

1. Introduction

In the territories that present social and public order conflicts, information management and timely access to it, is of vital importance as it contributes to the understanding of the nature of the conflicts that arise [1]. If we refer to an organization, according to B.S.I. Group (British Standards Institution), successful businesses understand the value of timely, accurate information, good communications and secrecy. Information security is as much about exploiting the opportunities of our interconnected world as it is about risk management. That's why organizations need robust information security management [2]. According to Pipkin, information security is the process of protecting the intellectual property of an organization [3]. All models related to the measurement of information security success are mostly driven by financial performance indicators, and not by psychological or other non-economic goals [8]. One durable and well-known way to achieve security for organizational information is through the implementation and then certification, through a certification body, of an ISMS - Information Security Management System, according to the international standard ISO/IEC 27001:2005, with its revised version in 2013. An *information security management system* is a set of managerial interconnected processes having the target to establish the right direction regarding information security in organization. It is important to stress the necessity of having an ISO/IEC 27001 certified organization. Why adopt an information security management standard? Organizations take into considerations at least two directions: an ISMS is a powerful market instrument so it is about *market assurance* and the second advantage refers to *governance*.

- The certified organization is able to provide confidence to all interested parties and within the market, it is able to assure the main functions of information security: availability, non-repudiation, authenticity, confidentiality and integrity of information.
- Regarding governance – how the organization is managed, by an ISMS the company acts in a proactive way to manage information security. An organization might choose to certify an ISMS for better management or to attract new customers.

The paper has the objective to propose a guide for adopting the ISO/IEC 27001:2013 standard in organizations (particularly from Romania), as a response to the results of a research made by the author in 2014. The research, based on a questionnaire with respondents from Romanian and Bulgarian organizations, revealed the intention of many organizations to be certified or recertified; so, there is a necessity of having

such a guide which is expected to have a wide applicability. The paper presents some aspects regarding the information security management system according to the new requirements of the ISO/IEC 27001:2013 international standard: new concepts, requirements and changes introduced in the standard etc. Then, based on the author exploratory research, the paper contributes with some new elements useful for organizations that have the intention to adopt an ISMS or to upgrade an existing one. The author is not aware about other references to this subject in Romanian literature. The remaining part of the paper is organized in 4 chapters devoted to the following issues, respectively: contributions of the ISO/IEC 27001:2013 standard, guide for adopting this standard, a case study – an example of practical use, and conclusions.

2. Contributions of the ISO/IEC 27001:2013 Standard

A new version of the standard for Information Security Management, ISO/IEC 27001 has been released in 2013. There are a lot of changes in the newer version of the standard, the most important of them are presented below:

Changes to the structure of the standard

The basic structure has been revised to align 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/IEC 9001, Quality Management Systems and ISO/IEC 14001, Environmental Management Systems [4]. The structure of the ISO/IEC 27001:2013 is as follows:

1. **Introduction** – the Plan-Do-Check-Act section has now been removed.
2. **Scope** – there is a stronger focus on risks management in order to achieve the objectives / needs of the organization.
3. **Normative references** – ISO/IEC 27001 is presented as the only normative reference, ISO/IEC 27002 was removed.
4. **Terms and definitions** - terms and definitions have been removed from the standard and reference is now made to ISO/IEC 27000:2012.
5. **Context of the organization** – news: the organization needs to determine internal and external issues, the needs and expectations of interested parties; the scope of the ISMS needs to consider the issues identified and the requirements of the interested parties; there is an explicit reference to ISO/IEC 31000:2009 regarding risk management.
6. **Leadership** - the previous Management Responsibility Clause is replaced by Leadership – this chapter is about the requirements to be met by the top management of the organization.
7. **Planning** – main features of this chapter are about information security risk assessment and treatment and information security objectives.
8. **Support** - requirements for determining and providing resources, and determination of competence, awareness and communication have little change from the previous version. Requirements for control of documents and records have been revised and the standard now refers to "documented information" [4].
9. **Operation** – this chapter requires planning, implementing and controlling processes to achieve objectives, performing risks assessments and implementing risk treatment plans [4].
10. **Performance evaluation** - main features of this chapter are about monitoring, measurement, analysis and evaluation, internal audit and management review.
11. **Improvement** – this clause now requires organizations to react to non-conformities and take action to control and correct them. Requirements to determine the causes of non-conformities and take action to eliminate them are essentially unchanged. The requirement to continually improve the ISMS has been expanded to include the suitability and adequacy of the ISMS as well as the effectiveness, as in the previous version [4].

Requirements for documented information

In the newer version of the standard the requirements for *documented procedures and*

records were replaced with requirements for *documented information*. The following documented information are mandatory for certification (see ISO/IEC 27001:2013 international standard [6]):

- 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)

The list of the new requirements

Listed below (the number of chapter in the standard): 4.2(a); 4.3(c); 5.1(b); 6.1.1(a); 6.1.1(b); 6.1.1(c); 6.1.2(a); 6.2(b); 6.2(c); 6.2(c); 6.2(f); 6.2(g); 6.2(h); 6.2(i); 6.2(k); 7.3(a); 7.4(a); 7.4(b); 7.4(c); 7.4(d); 7.4(e); 7.5.1(b); 8.1; 9.1(c); 9.1(d); 9.1(f); 9.3(c)(4); 10.1(a); 10.1(a)(1); 10.1(a)(2); 10.1(e); 10.1(f).

Some requirements were eliminated

(selection):

- 4.2.1(i) the necessity of having the management authorization for the implementation and the operation of ISMS;
- 8.3(d) the results of the records for taken actions;
- 8.3(e) the revision of the taken preventive actions;
- 8.2 the documented procedure for corrective actions must define requirements in this direction;
- 8.3 the documented procedure for preventive actions must define requirements in this direction.

Changes related to the list of measures in the Annex:

The number of measures in the Annex of the standard was reduced from 133 to 114; the number of sections increased from 11 to 14 as a consequence of the introduction, deletion or fusion of some measures. The sections from the new Annex of the standard refers to (selection):

- the human resources security;
- the policy of information security;
- the access control;
- the cryptography;
- the information security incidents management;
- the asset management;
- the communication security;
- the security of operations.

3. Guide for Adopting the ISO/IEC 27001:2013 Standard

This guide was meant to help Romanian organizations interested in adopting the new version (from 2013) of the ISO/IEC 27001 standard. If we refer to an organization that has no ISMS implemented, adopting the ISO/IEC 27001:2013 means the achievement of the requirements presented in the standard. If we refer to an organization that has already implemented an ISMS, a transition guide from version A (ISO/IEC 27001:2005) to version B (ISO/IEC 27001:2013) of an international standard will help the company to understand the relation between the two analyzed entities. There are also important aspects that need to be emphasized in relation with this transition process (some aspects are based on [2]), for example: the steps / improvements that an organization needs to follow in order to achieve the requirements of the new standard and the impact that the new version of the standard is likely to have on the existing ISMS.

Aspects regarding the applicability of this proposed guide are presented in chapter 4, as a case study example.

The guide has 2 main parts:

1. The analysis of possible strategies

According to [2], there are at least two possible strategies in this respect (see Figure 1):

- A ***"make-over"*** strategy – this strategy implies the minimum necessary changes to the existing ISMS (processes and existing documentation);
- A ***"fresh look"*** strategy – this strategy implies a completely fresh look for the ISMS according to the new version of the standard, ISO/IEC 27001:2013.

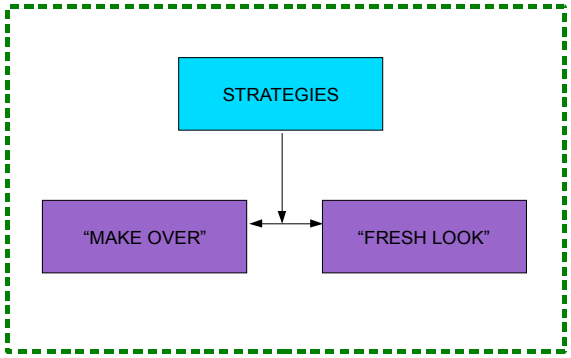

Figure 1. Two possible strategies

A transition strategy – "make over" (concrete steps and the allocation of resources) will help the organization to understand the relationship between ISO/IEC 27001:2013 and its predecessor, ISO/IEC 27001:2005.

The implementation of the new standard requirements can be done quite quickly. According to [2], given the improvements of ISO/IEC 27001:2013 over its predecessor, organizations are encouraged to start transition as soon as they can rather than postpone it to the latest possible time. Organizations need to decide whether to:

- highlight them as opportunities for improvement with the intention of making the changes at an appropriate time in the future; or
- make the changes immediately.

For the *„make over"* strategy, the concrete actions that are to be taken are described in the next section, 2. For the *„fresh look"* strategy, the most suitable guide is the new version of the standard itself. For both strategies, it is important the allocation of all necessary resources.

2. The implementation of the selected strategy

In both strategies the first step is a serious analysis of the organization. If the company has adopted the ISO/IEC 27001:2005, the analysis is done between the existing ISMS and the new version of the standard. Knowing how the existing ISMS conforms to the previous standard will help the organization to establish tasks for transition. This section describes the actions that are to be taken by the organization, steps suitable for the "*make over"* transition strategy.

There are two subsections:

- issues where the changes may be minimal;
- (possible) challenges - issues related to the new requirements presented in the ISO/IEC 27001:2013 version of the standard.

Regarding clause 7.5, all changes to the existing documented information should be recorded.

The main issues where the changes may be minimal are the following:

- Regarding **documented information**, it is a new term that replaces the terms *documents* and *records* - the change is minimal;
- Regarding the **policy** – in the new standard the *information security policy* (clause 5.2), not *the ISMS policy* is required; there is also a requirement (clause 6.1.2) that refers to the establishment and maintain the risk criteria. If the previous ISMS policy of the organization contains the two above requirements, no changes are required to the policy. There is no requirement to change the name of the policy. There are other requirements that are to be met in the policy [2]:
  - The criteria for performing information security risk assessments (see Clause 6.1.2 a) 2));
  - The organization's policy towards releasing its information security policy to interested parties (see Clause 5.2 g)); and
  - The organization's policy regarding external communications (see Clause 7.4).

- There are also two requirements that concern "commitment", see Clauses 5.2 c) and d);

- Regarding the **terms of reference for top management** - a change may be required to accommodate the specific responsibilities given in clauses 5.1 a) to h) [2];
- Regarding **the risks management** - as a new element, ISO/IEC 27001:2013 uses the vocabulary of ISO/IEC 31000 - Risk management – principles and guidelines, and refers to consequences rather than impacts. In the new version of the standard there are no additional requirements regarding the risk management process; so, minimal or no changes are necessarily;
- Regarding the **awareness** - a change may be required to accommodate the requirements of clause 7.4 as the process of creating awareness may be regarded as a form of communication [2];
- Regarding the **corrective actions** - the existing procedures need to be reevaluated and strengthened in order to have an accurate treatment of nonconformities;
- Regarding the **scope of the ISMS** – the organization can rethink the scope of its ISMS in order to add other entities (e.g. external risk sources) that were previously excluded. This rethink may be done by the organization in order to demonstrate conformance with the clause 4.3;
- Regarding the **responsibilities** - a change may be required to accommodate the specific responsibilities given in clauses 5.3 a and b [2];
- Regarding the **improvements** – the procedures for improvements are to be reevaluated in order to cover suitability, adequacy and effectiveness of the ISMS;
- Regarding **the information security objectives** - if an organization considers its information security objectives as being timeless policy objectives, the requirement of clause 6.2, which refers to 'relevant functions and levels', may come as a shock. However, it may only require a change to the way conformance is described. It is likely that an organization already sets objectives at all relevant functions and levels, and it is only a question of recognizing that it does this and describing how. For example, it is good practice when placing actions to define objectives, assign responsibilities and set targets dates for completion. If an organization already does this, then it already conforms to this clause [2];
- Regarding **The Statement of Applicability (SOA)** – the Annex A has been changed in the new version of the standard so, the Annex A controls are different from the previous version. In this new context, the SOA must be updated.
- The main (possible) challenges - issues related to the new requirements in the ISO/IEC 27001:2013 are as follows:
- Regarding the **communication** – it is about the clause 7.4 that is more specific than in the previous version of the standard, but the new requirements are related to the common practice, so, it is probably that these new requirements to be already achieved by the organization;
- Regarding the **integration** – according to [2], clause 5.1 b) requires top management to ensure integration of the ISMS requirements into the organization's business processes. If the business functions of an organization were to be represented by a set of one or more workflow diagrams and therefore the activities that correspond to the ISMS requirements are spread throughout these work flows, then the integration requirement is probably met. However if the ISMS requirements are contained in a single workflow which contains nothing else, then the integration requirement is probably not met. In the first case, it is then a question of how best to demonstrate conformance. If workflow diagrams exist, or can be visualized, e.g. through a software interface, then that would be an easy way to demonstrate conformance. If the integration requirement is not met, then the workflow concept may provide a route to achieving conformance [2];
- Regarding the **stakeholders and their requirements** – in accordance with the clause 4.2, an organization *must* determine the interested parties, – e.g. customers and suppliers (and their requirements – e.g. documented in contracts, purchase orders etc), that are relevant to the ISMS. This new requirement may be already satisfied in organization, the identification where this information (regarding interested parties and their requirements) is

documented is all that the organization should be done;

- Issues (based on [2]):
  - An important issue would be *those concerned with information security*. If these are unknown or the organization is uncertain of them, it may be possible to reverse engineer them from a consideration of the information security policy, objectives and the information security risk assessment and risk treatment;
  - Another important issue refers to *the motivation of the organization for having an ISMS* - the motivation may have changed over time and the organization should reflect on that;
  - Other issues, which are likely to have been already addressed by an organization would relate to *the operation of the ISMS*, such as *management commitment and staff motivation*. Finally, organizations should consider looking through management meeting minutes and its records of preventive actions for further issues. After all, clauses 4.1 and 6.1.1 are the new way to deal with preventive action;
- **Monitoring, measurement, analysis and evaluation -** the requirements of clause 9.1 are more detailed and exact than the requirements for the ISMS and control effectiveness in ISO/IEC 27001:2005. From the perspective of transition it may be best to start with a clean sheet of paper [2];
- **Actions to address risks and opportunities (general) -** existing preventive action procedures will need to be revised or replaced to ensure conformance with clauses 4.1, 4.2 and 6.1.1 [2].

4. Case Study – an Example of Practical Use

The proposed guide is especially suitable for organizations (all types and dimensions) that already have implemented (and certified) an ISMS according to ISO/IEC 27001:2005 and want to achieve the new requirements of the ISO/IEC 27001:2013. The guide is not an exhaustive one, it is very difficult to do that. All organizations are different and this guide needs to be interpreted in the context of the individual needs of each organization. The guide highlights the most important changes that an organization should make in order to achieve the new requirements of the ISO/IEC 27001:2013. It can be also considered for more organizations a starting point in achieving the requirements of the new international standard for information security management, ISO/IEC 27001:2013. The main steps that an organization should follow in order to achieve the ISO/IEC 27001:2013 requirements are presented in the Figure 2 and analysed below.

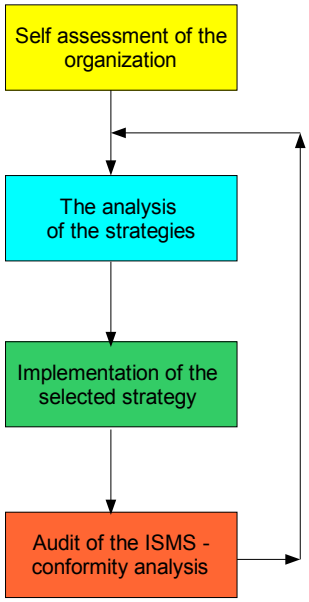

Figure 2. The steps for adopting ISO/IEC 27001:2013

Below there are presented only steps 1 and 4 because steps 2 and 3 were detailed in the previous section. It is also useful for an organization to be aware of the correlation between the business risks and features & advantages of the ISO/IEC 27001 standard. Such an analysis (based on [5]) is presented in Table 1.

Self-assessment of the organization

The assessment, through a model, of the company's readiness for an ISO/IEC 27001 Information Security Management System is the first step before the implementation and certification of an ISMS. The proposed model (details are provided in [7]) is especially suitable for organizations (all types and dimensions) that already have implemented (and certified) an ISMS according to ISO/IEC 27001:2005 and want to achieve the new requirements of the ISO/IEC 27001:2013, or

have the intention to implement and certify an ISMS according to ISO/IEC 27001:2013. The model is not an exhaustive one, it is very difficult to do that. All companies are different and this model needs to be interpreted in the context of the individual needs of each company. The model is presented in the Figure 3 (details are provided în [7]) and consists of the following modules:

- LEADERSHIP – evaluated with 19P (points) – for example there are 5 points for „Are the required resources to establish, implement, operate, monitor, review and improve the ISMS determined and provided?"
- PLANNING – evaluated with 18 points – for example there are 3 points for „Is there an approved information security policy?"
- SUPPORT – evaluated with 5 points for „Are the documented information - documents and records, related to the information security management system managed and controlled according to defined procedures?"
- OPERATION – evaluated with 17P – for example there are 4 points for „Is there a risk treatment plan (actions, resources etc) for managing information security risks?"
- PERORMANCE EVALUATION – evaluated with 15 points – for example there are 3 points for „The internal ISMS audits are conducted at planned intervals"
- IMPROVEMENT – evaluated with 6P – for example there are 3 points for „Are appropriate corrective and preventive actions identified and implemented?"
- SECURITY CONTROLS – evaluated with 20 points – for example there are 3 points for „Information security risks from external parties are identified by the organization".

Regarding the level of readiness, some thresholds can be proposed as follows [7]:

- 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.

Based on considerations presented in [7], an organization can be in one of the following situations:

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

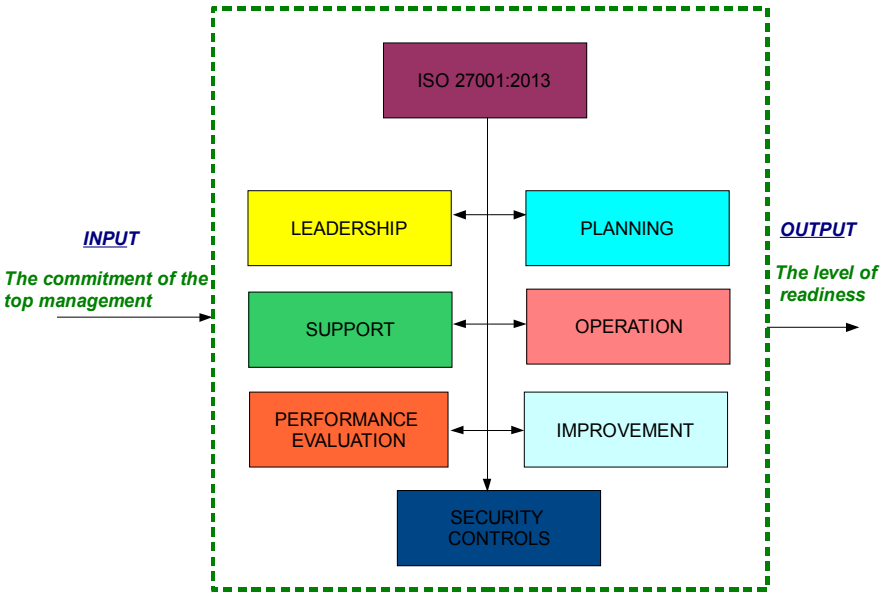

Figure 3. The preliminary model to assess the company's readiness for an ISO/IEC 27001 ISMS

level of readiness) the requirements of the new standard;

2. 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/IEC 27001 process (related to the requirements of ISO/IEC 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.

Audit of the ISMS – the conformity analysis

The audit is the conformity evaluation. After the ISMS (transition) guide is applied, an audit in order to see if the new requirements of the standard ISO/IEC 27001:2013 have been achieved is necessarily. The main stages of a typical audit assignment are as follows [9]:

1. **Scope** - During this phase, the ISMS auditors determine the main area/s of focus for the audit and any areas that are explicitly out-of-scope, based normally on an initial risk-based assessment plus discussion with those who commissioned the ISMS audit.
2. **Plan-** The output of this phase is the (customized) audit workplan / checklist and

Table 1. The correlation between business risks, features of the standard and advantages

Business risk	Feature of the standard	Advantages (how will the standard help)
The protection of customer information - failure.	Procedure for the identification of relevant risks, understanding of how the risk is formed and evaluation of improvements	✓ Better awareness and understanding of risk applicability. ✓ Better risk management. ✓ Fewer incidents
Damaged reputation from information breach – the decrease of the number of customers and investors	Operational controls to be in place	✓ Reduced incidents and accidents and a better management of them.
1. Insufficient understanding of business 2. Threats to the business.	1. The necessity of a trained and competent staff. 2. The necessity of worker communication, participation and consultation in the ISMS. 3. Roles / responsibilities need to be defined.	✓ Staff are aware of their roles and responsibilities in looking after their own information security. ✓ Staff are more likely to spot and avoid potential hazards. ✓ Less time lost through incidents.
Interruption to internal operations as a result of IS procedures.	1. Operating controls to be in place. 2. Procedures for overview and testing to be in place.	✓ Less likely to have an incident. ✓ Better prepared for incidents: quicker response and reduced / minimum impact. ✓ More efficient (in) operations.

an audit plan agreed with management.

3. **Fieldwork** - During the fieldwork phase, audit evidence is gathered by the auditor/s working methodically through the workplan or checklist, for example interviewing staff, managers and other stakeholders associated with the ISMS, reviewing ISMS documents, printouts and data (including records of ISMS activities such as security log reviews), observing ISMS processes in action and checking system security configurations *etc*.
4. **Analysis** - The accumulated audit evidence is sorted out and filed, reviewed and examined in relation to the risks and control objectives.
5. **Report** - The output of this phase is a completed ISMS audit report, signed, dated and distributed according to the terms of the audit charter or engagement letter.
6. **Close** - In addition to indexing and cross-referencing and literally shutting the audit files, closure involves preparing notes for future audits and following up to check that the agreed actions are in fact completed on time.

The following normative documents can be used in an audit process:

- **ISO/IEC 27000: 2014** - It contains an
- overview of the ISO27k standards and a vocabulary or definition of terms common to many of the ISO27k standards;
- **ISO/IEC 27001:2013** - Information
- technology-- Security techniques -- Information security management systems – Requirements;
- **ISO/IEC 27002:2013** - Information
- technology-- Security techniques -- Code of practice for information security controls - Provides more pragmatic guidance than 27001 on how to design, implement, manage and improve an ISMS;
- **ISO/IEC 27006:2011** - Information
- technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems;
- **ISO/IEC 17021:2011** - Conformity
- assessment--Requirements for bodies providing audit and certification of management systems;
- **ISO 19011:2011 -** Guidelines for auditing
- management systems.

According to Figure 2, if the analysis reveals that there are unfulfilled requirements, a rethink of the (transition) strategy can be done until all the issues required by the standard are achieved.

5. Conclusions

Information security is a sensible and very important pillar in achieving protection, stability, predictability and finally profit in an organization. An organization may initially choose to have an ISMS in order to inspire confidence within the marketplace. Once it has its ISMS, as it matures, the people within the organization often experience the benefits of being able to better manage information security [2]. An organization has also the interest to achieve this goal and protect itself in order to assure in company a framework for development and profit. In the context of a new version of the international standard on information security management systems, this paper helps an organization to adopt the ISO/IEC 27001:2013 international standard or to make easier the transition from ISO/IEC 27001:2005 to ISO/IEC 27001:2013. The core of the paper is the guide for adopting the ISO/IEC 27001:2013 standard, as well as the proposed methodology to implement the guide with a preparatory phase (organization readiness self-assessment) and a final conformity analysis (ISMS audit).The approach can help organizations to have an example of practical use. Further work will be devoted to build a pilot implementation of the proposed approach.

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. RIBON R. J., GARCIA VILLALBA L.J., KIM T., **Application of Mobile Technology in Virtual Communities with Information of Conflict-Affected Areas**,

Studies in Informatics and Control, ISSN 1220-1766, vol. 22(1), pp. 33-42, 2013.

2. BREWER, D., **Moving from ISO/IEC 27001:2005 to ISO/IEC 27001:2013**, BSI Report, BSI Group, 2013.
3. [3] PIPKIN, D. **Information security: Protecting the global enterprise.** New York: Hewlett-Packard Company, 2000.
4. **New ISO/IEC 27001:2013 Information Security Management Systems,** SAI Global report, 2013.
5. **ISO/IEC 27001 Information Security - Features and benefits,** BSI Group report, 2009.
6. **ISO/IEC 27k family of standards** (http://www.iso.org/iso/).
7. ȚIGĂNOAIA, B. **A preliminary model to assess the company's readiness for an ISO/IEC 27001 Information Security Management System,** Intl. Conf. Comm, Context and Interdisciplinarity, 3rd edition, Tg. Mures, Romania, 23-24 October, 2014, pp. 279-287.
8. HUMPERT-VRIELINK, F,. N. VRIELINK, **A Modern Approach on Information Security Measurement.** Proceedings of the 14th Information Security Solutions Europe Conference-ISSE 2012; Brussels, Belgium, October 23-24, 2012, pp. 48-53.
9. HINSON G. ET ALL, **ISMS Auditing Guideline**, ISO27k Implementers' Forum, 2008.