DE GRUYTER OPEN

DOI: 10.1515/aucts-2015-0036

ACTA UNIVERSITATIS CIBINIENSIS – TECHNICAL SERIES
Vol. LXVI 2015

INFORMATION SECURITY MANAGEMENT - PART OF THE INTEGRATED MANAGEMENT SYSTEM

MANEA Constantin Adrian
Faculty of Electrical Engineering and Computer Science/Department of Automation and Information Technology, "Transilvania" University, Brașov, Romania, a.c.manea@unitbv.ro

Abstract: *The international management standards allow their integrated approach, thereby combining aspects of particular importance to the activity of any organization, from the quality management systems or the environmental management of the information security systems or the business continuity management systems. Although there is no national or international regulation, nor a defined standard for the Integrated Management System, the need to implement an integrated system occurs within the organization, which feels the opportunity to integrate the management components into a cohesive system, in agreement with the purpose and mission publicly stated. The issues relating to information security in the organization, from the perspective of the management system, raise serious questions to any organization in the current context of electronic information, reason for which we consider not only appropriate but necessary to promote and implement an Integrated Management System Quality - Environment - Health and Operational Security - Information Security*

Key words: international standard, management system, information security, control, integrated

Introduction

In the preparation of the launching in September 2015, the new edition, the fifth, of ISO 9001: 2015 standard - the Quality Management System -standard currently with the most worldwide application both considering the number of certified organizations - over 1.1 million worldwide - as well as geographical and political coverage - more than 100 countries took over identically the ISO 9001 standard: 2008, former ISO 9000: 2000 - an integrated approach within the internal management system of an organization of the international quality standards, ISO 9001 for the quality management systems (QMS), ISO 14001 for the environmental management systems, OHSAS 18001 for the health and occupational safety management systems, ISO 27001 for the information security management systems (ISMS) is a necessity imposed by the competition on the production and sales markets, but also an internal necessity to eliminate responsibilities and inappropriate relationships or those backed by individual procedures.

Starting from a Quality Management System (QMS), certified in an organization, overlapping certain procedures and adding some specific processes necessary for environmental management systems and / or health and occupational safety or security of information you can obtain an Integrated Management System (IMS), which will bring added value to the organization and its products / services. This option, which can be analyzed and adopted at the top level of management, is based on the existence of certain common processes to each of ISO 9001 (QMS), ISO 14001 (EMS) ISO 27001 (ISMS) and OHSAS 18001 standards, respectively processes regarding the control of documents, the education and training of the personnel, internal audit, management analysis and establishment of corrective and preventive actions in the area covered by each of the mentioned standards.

Aside from the easiness of the integrated approach of the management system, we must take into account the benefits of the organization by developing its Integrated Management System, advantages among which we enumerate demonstratively: the cost reduction on the individual implementation and certification of management systems; coherent and correlated planning of the activities of the organization and the establishment of overall strategies by taking into consideration the aspects regarding quality, environment, health and safety at work, information security, social responsibility and business continuity; optimizing the decision-making process in accordance with the determination of the necessary resources.

Thus, if in terms of organizational development, the integrated approach of the Management System provides increased profits and risk reduction, focusing attention on the organization's objectives from the employees' perspective, the benefits brought are to be found in the improved internal

communication and the development of instruction and staff training. The integration of an information security management system in the Integrated Management System of an organization is necessary, in the

20st century due to the development of information technology and the strong dependence on the communication of information within the organization, but also externally, through computer systems, under the development of communication infrastructure at internal level - Intranet - global connection - the Internet. From this perspective, this paper aims to present arguments that favour the implementation of integrated systems of the management systems (quality and / or environment - information security).

2. The Management System

Each company and organization with its specific activity is unique as identity and internal organization, for which the management system is individualized. Regardless of the size of the organization, the core business and market position, designing and developing a proper management system is necessary in order to communicate the interdependence of people and processes in view of decision-making, based on accurate and real analysis, aimed at raising the profit and competitiveness within the organization.

Any management system has four main elements that are found in international standards:

- Policy and management objectives
- The management responsibilities so that each employee of the organization knows the needs and requirements of the position occupied
- Defining the internal processes and procedures that ensure the organization's objective
- The distribution and analysis, under the form of internal documents and records in order to improve the performance of the organisation.

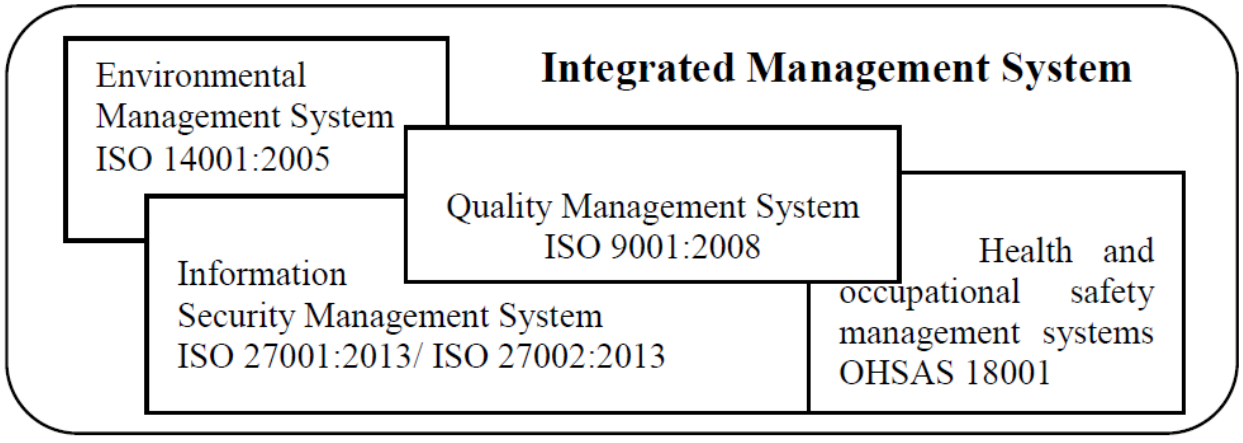
We find that no matter of the management system approached, an important element is the data being operated in that system, data which takes the form of written or electronic documents that have a well-defined circuit and an accessibility established through procedures and processes characteristic to the management system. Thus, the need for control and data security is defined and regulated by the management system, regardless of the standard involved, for which the correlation and integration of the standard regarding the Information Security Management System (ISMS) ISO 27001: 2013 and ISO 27002: 2013, together with the ISO 9001 regarding the Quality Management System (QMS) in an Integrated Management System directly benefits any organization.

3. The Integrated Management System

The Integrated Management System means that several management systems are united under a common structure to simplify documentation, to facilitate auditing, certification and to channel their synergistic effects [1].

In a graphical approach as in Figure 1., the Integrated Management System provides the planning of the objectives and processes necessary in order to obtain results consistent with the organization's strategy and the requirements / expectations of customers, implements the processes under safety conditions concerning the circulation of information and data, verifies, through specific indicators each management system, the processes and the product obtained in accordance with the policies, objectives and requirements on product quality, and takes actions to improve the performance of processes based on the results of internal audit.

Figure 1: The Integrated Management System



Addressing an Integrated Management System starts from two fundamental premises: at the core of trade is the organization's products and customers, on the one hand, on the other hand, the management systems serve to improve the planning, monitoring and analysis of managerial processes, for which the integrated management is the complex process of combining the resources with the organization's own
activities of planning, organizing, directing and controlling with the view to develop the organization's overall strategy and to achieve its goals on the long term.
To simplify and facilitate the separate implementation, operation and certification of quality (QMS), environment (EMS) and occupational health management systems, given that the three systems have common points, in Annex 1 OHSAS 18001: 2007 correspondences are specified between ISO 9001: 2001 (Quality), ISO 14001: 2005 (environment) and OH SAS 18001: 2007 (Occupational Health), regarding the requirements for each separate clause without a standard being regulated for an integrated implementation of the three management systems.
Although there are no regulations or international certification and implementation standards of an Integrated Management System, considering that various organizations have currently approached the concept of integrated management in terms of Quality Management System (QMS), Environment Management System (SMM) and / or Management System of Health and Occupational Safety (SMSSM), starting from the organization's needs to ensure the quality of products and the compliance with the customers' requirements under the general conditions imposed by the current society for environmental safety and by the legal framework regarding the employees' security at work, we believe that the inclusion into the overall management system by partial integration, of the Information Security Management System is imperative in the current information society.
If an integrated approach to Quality Management System -Environment -Health and Occupational Security - Information Security is facilitated by the similarities of the approaches on the four areas, in the sense that each of the four individual standards considers the concept of *prevention* and places the human factor involved at the heart of the specific processes of construction, implementation and operation of the management system, the option for the implementation of a completely or partially integrated system belongs to each organization based on the analysis of advantages and disadvantages of starting an implementation activity, starting inclusively from the duration (average of two years) of such a process.
If an organization has implemented and certified a Quality Management System, implementing an environmental management system and / or one of health and occupational safety may be based on the structure already in place through the development of those processes and procedures existing in the adjacent system. Regarding the Information Security Management System, a system Integration Quality Management is also facilitated by the existence of the product management and the product data management, components of the Quality Management, for both management systems - Quality and Information Security - provide a competitive advantage by meeting the contractual requirements regarding the product offered to customers, while demonstrating that information security, including that relating to the product and / or the customer is paramount for the organization.
The way in which the integrated system can be implemented varies from one company to the other. The characteristics of various organizations, such as the type of firm, the size, nature and complexity of its activities, the products and services performed, result in a certain structure of the management system implemented. The implementation and performing of the activity in an integrated system is a cyclical process, any activity ending with the measurement and auditing processes in order to improve operations.

4. An Integrated Quality Management System - Information Security

ISO 9001: 2008 standard, which is currently under revision procedure, the fifth version - edition 2015 includes requirements for developing their own internal procedures that cover all key areas of the organization, starting from the seven principles restructured in 2015 edition: orientation towards the customer, organizational leadership, employees engagement, procedural approach, improving the activity, making decisions based on the management relationship, including the relationship with the suppliers.
ISO 9001 Standard: 2008 promotes the adoption of a process-based quality management in developing, implementing and improving the effectiveness of the QMS in order to increase customer satisfaction by fulfilling its requirements to the product.
Since the twentieth century some authors [2] defined the quality management system as a "combination of equipment, software, specialists and procedures with a structure chosen in such a way as to facilitate the achievement of the objectives derived from the quality policy"
The Certification of Quality Management System (QMS) ISO 9001 does not guarantee the quality of the final product or service of the organization, but only ensures customers that there are quality processes

occurring in the production and / or supply of service that ensures customer satisfaction. Monitoring the internal processes and the verification for failures, ensuring the human resources security and the control on production processes, guarantees provision of corrective and preventive measures in a management system subjected to improvement by the final assessments and the internal audit, already established and implemented.

In organizations, the information is a very important resource for making management decisions, but not only in this respect. Compared with human resources, for example, information is endless, is produced and consumed quickly. The effectiveness and efficiency of an organization depend on the information available to it [3].

The series of ISO 27000 (ISMS) standard proposes ensuring information security and data protection in whatever form it exists (magnetic, optical, paper, etc.) by implementing a set of policies, practices, procedures, organizational structures and software functions [4]. The certification of Information Security Management System guarantees the customers and business partners of the organization that information risks are controlled and that the information received and that provided by the organization is protected against threats and vulnerabilities, the information security maintaining the following properties: availability, integrity and confidentiality. An ISMS is a management system based on an approach of risks to which the organization is exposed and aims to establish, implement, operate, monitor, review, maintain and improve the information security.

Addressing this standard provides long-term security based on the implementation of policies, procedures and security methods in order to protect the information and resources of the organizations. By minimizing the cyber risk, there is a guarantee that the management system is functional and meets the operational requirements of the company, the customer expectations and it complies with the legislation.

The Information Security Management System (ISMS) involves both hardware and software equipments from the organization, as well as all the staff of an organization with access to the information system, as well as the third parties outside the organization whose access must be controlled permanently.

In the statistical reports [3], [5] it is confirmed that information security experts maintain:

- the information security depends on people more than on technology;
- the information security is like a chain - is as strong as its weakest link;
- the employees represent a greater threat to the security of information than those outside the organization;
- the information security is not a status, but a process that requires a continuous dynamic;
- the information security is not a technical chapter, often information security management is very important.

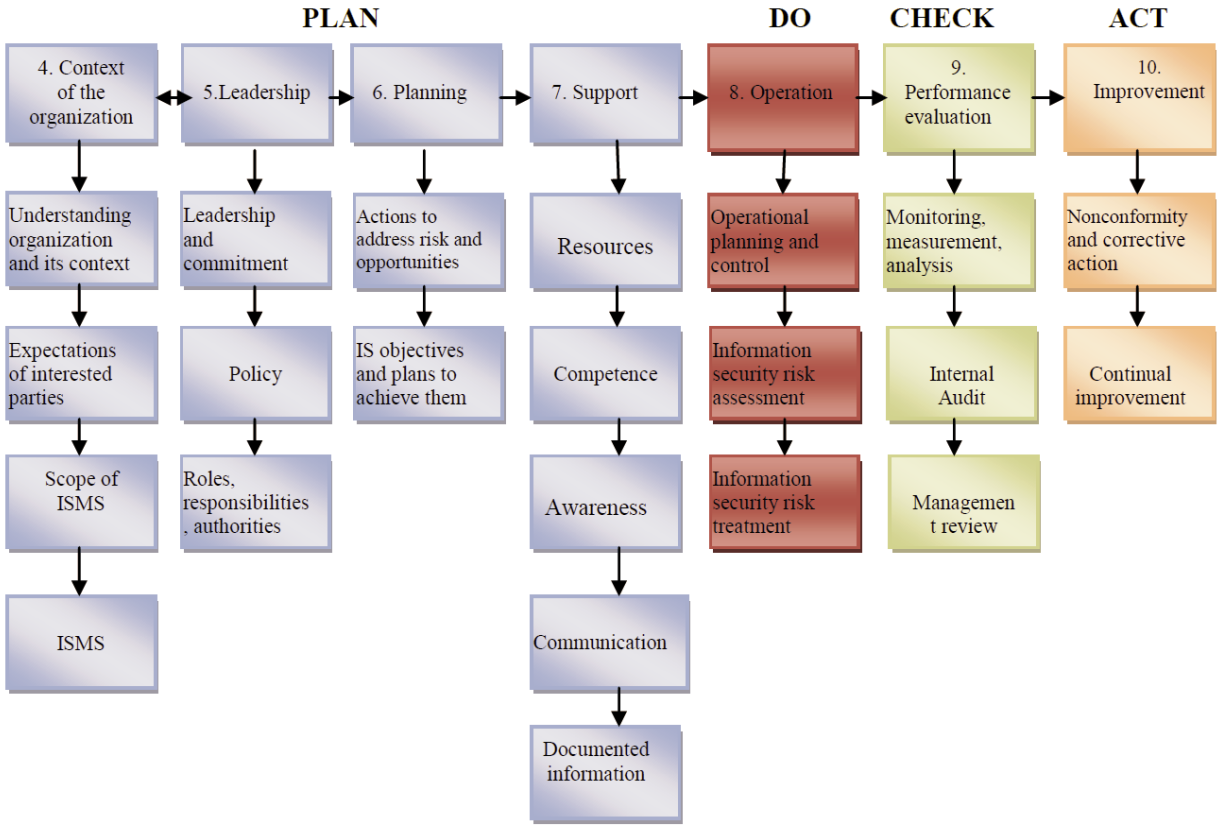
ISO / IEC 27000 family (in short "ISO27k") includes common safety standards published in common by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Given the dynamic nature of security information, SMSI concept incorporates a continuous feedback and the improvement of activities according to the Deming PDCA cycle as (plan-do-check-act) of continuous approach.

ISO / IEC 27002 standard, the former standard ISO / IEC 17799 which has been renamed in order to be part of ISO 27000 series dedicated to information security, establishes the general principles for initiating, implementing, maintaining and improving the information security management in an organization. ISO / IEC 27002 standard contains the best control practices in the information security management areas:

- The Security Policy;
- The organization of information security;
- The management of assets;
- The human resources security;
- The physical and environmental security;
- The communications and operations management;
- The access control;
- The acquisition of information systems, their development and maintenance;
- The management of information security incidents;
- The business continuity management.

ISO/IEC 27003 focuses on the critical aspects necessary for the successful design and implementation of an information security management system (ISMS) in accordance with ISO/IEC 27001, describing the design and specifications for an information security management system from the initiation until the accomplishment of the implementation plans.

Figure 2: The ISO 27001: 2013 Structure



Source: B.S.I. Group

The new version of ISO 9001: 2015 standard will also bring structural changes following the current structure of the standard to be developed on an identical structure, of 10 chapters, to the current structure of ISO 27001: 2013, which will be an additional argument to the implementation of an Integrated Management System ISMS QMS.

Even if the implementation of an integrated system benefits the organization and its activity, starting from the characteristics of each organization (size, number of employees, field, etc.) and questions such as: *What can be found in the organization regarding information security? , What should be improved?* and *What is missing and should be added?*, the process of integrated implementation of information security management must begin with a preliminary analysis which is to provide information on the state of the organization at a time.

The preliminary analysis should be undertaken by the team designated to implement the integrated system, who, thus establishing the existing facilities and the regulations in force on the product/service offered, the procedures and internal processes applied, which may be regulated by the existence of a quality management system implemented and certified in the organization, identifies and assesses the risks affecting the movement and security of information and the information systems used in the activity and their impact on the activity in general and in particular on the product quality.

Conclusions

Information security is an area that every organization must deal with very carefully at top level management, as it represents a core pillar which really is not bringing immediate and direct profit, but contributes significantly to the achievement of organizational goals, and indirectly contributes to getting profit.

Given that, as mentioned above, there is no national or international regulation or standard covering the Integrated Management System, taking into account the factual situation of the organizations that, in recent years, have opted and promote the System Integrated Management, it follows that the need to develop an integrated system is imposed from within, not from the external environment.

Even if you cannot say that there are universal rules regarding the establishment *a priori* of the relationship in which the management systems must be put in an integrated structure, however, for the guidance of the process of adopting the suitable solution in an organization, the following recommendations can be formulated:

a. The organization must establish a relationship as objective as possible between the importance of the environmental and / or informational security and / or occupational health and safety aspects, on the one hand, and the quality assurance aspects, on the other hand;
b. The adoption of the decision to achieve an integrated management system - quality - environment / health and occupational safety / security of information must be based on the analysis of the essential reasons underlying the decision to implement each of the management systems from the perspective of the organization;
c. The decision to implement or not an integrated management system must be based on the analysis of similarities and differences between management systems chosen, as well as the advantages and disadvantages of a possible integration. It is particularly important that following the analysis performed, the organization formulate a personal point of view that takes into account its particularities.

One of the most commonly adopted solutions that we support is the one regarding the integration of the quality management systems and one or all the other management systems (EMS, ISMS, SMSSM) in a variant of partial integration, very flexible and adaptable to a large number of situations. According to this, the global management system has a coordination unit at the peak, from which emerges a mixed quality structure - environment - information security - occupational safety and health based on separate handbooks and on a combined system of procedures and other documents, partially integrated .From case to case, the joint and separate parts can be developed or reduced, without this interaction between systems being affected substantially.

Regardless the management systems that an organization wants to implement in an integrated system, the following processes should be common to all systems:

- The control of documents;
- The control of records;
- The Internal Audit;
- Management analysis;
- Corrective actions;
- Preventive actions.

ACKNOWLEDGEMENT: *This paper is supported by the Sectorial Operational Programme Human Resources Development (SOP HRD), ID134378 financed from the European Social Fund and by the Romanian Government.*

References

- Avram S.E., The implications of implementing an integrated system of management in an organization, The Symposium the Impact of the community Acquis on the environment equipment and technologies, (2009). (available on http://www.inginerie-electrica.ro/acqu/pdf/2009_s2_l1.pdf accessed 15.01.2015)
- Ionescu, S.C., Industrial excellence - theory and practice of quality, pp.378, Economic Publishing House, Bucharest (1997).
- Ţigănoaia B., Theoretical and practical considerations regarding the information security management system within organizations in concordance with the new international standard ISO / IEC 27001: 2013 Globalization, Intercultural Dialogue and National Identity, pp.62 - 68, Targu Mures, Romania (2014).
- ISO / IEC 27002: 2005 Information technology - Security techniques - The Code of practice for information security management
- E.N.I.S.A. Country Reports, 2008 http://www.enisa.europa.eu (accessed 15.01.2015).
- B.S.I. Group : https://bsiedge.bsi-global.com/newiso27001/ (accessed 23.02.2015).