**Josip Britvić, univ.spec.oec.**
Virovitica college
Matija Gupca 78, 33000 Virovitica
Phone: 033/721-099 Fax: 033/721-037
E-mail address: josip.britvic@vsmti.hr

**Anita Prelas Kovačević, dipl.oec.**
Virovitica college
Matija Gupca 78, 33000 Virovitica
Phone: 033/721-099 Fax: 033/721-037
E-mail address: anita.prelas.kovacevic@vsmti.hr

**Monika Cingel**
Virovitica college
Matija Gupca 78, 33000 Virovitica
Phone: 033/721-099 Fax: 033/721-037
E-mail address: monikacingel@gmail.com

# INTEGRATION POSSIBILITIES OF ISO 9001:2008 QUALITY MANAGEMENT SYSTEM WITH ISO 27001:2010 INFORMATION SECURITY MANAGEMENT SYSTEM

# MOGUĆNOST INTEGRACIJE SUSTAVA UPRAVLJANJA KVALITETOM ISO 9001:2008 I SUSTAVA UPRAVLJANJA INFORMACIJSKOM SIGURNOŠĆU ISO 27001:2010

## *ABSTRACT*

*The requirements of customers, users of services and actions of competitors require companies to constantly raise the level of quality of products and / or services as well as the quality level and functioning of organization. Other requirements like those arising from legislation, requirements of local communities and environment also require organizations to adapt. To help organizations meet all these requirements they can use existing tools such as ISO 9001, ISO 14001, ISO 27001 and other standards. By integrating multiple ISO standards into one integrated system it's possible to meet a wider range of requirements. The paper analyzes the possibility to integrate the ISO 9001:2008 quality management system with ISO 27001:2010 Information Security Management System and application possibilities of the integrated system in practice. Organization with implemented quality management system proves that its quality management system complies with the requirements of ISO 9001:2008. Thus the risk of uncertainty in customers towards the quality of products or services is reduced, so organizations are increasingly seeking to obtain this certification. As some organizations require not only the quality of products and services, but also the safety of these, ISO 9001:2008 is a great start for organizations towards implementation of other ISO standards, in this case the ISO 27001:2010. The purpose of ISO 27001:2010 is to show customers that information security in the organization is carried out in the best possible way and to gain their trust. Therefore we can say that the ISO 27001:2010 means for information security the same thing as ISO 9001:2008 means for quality management system. In this paper will be shown how to implement the standards individually and whether there is the possibility of integrating these standards.*

***Key words**: ISO 9001, ISO 27001, integrated systems, information security, quality management*

### *SAŽETAK*

*Zahtjevi kupaca i korisnika usluga, te potezi konkurenata zahtjevaju od poduzeća da konstantno podižu razinu kvalitete proizvoda i/ili usluga ali i razinu kvalitete ustrojenosti i funkcioniranja svoje organizacije. Isto tako, ostali zahtjevi kao što su zahtjevi koji proizlaze iz zakonske regulative, zahtjevi lokalne zajednice i okoline traže od organizacija da se prilagode. Kako bi organizacije zadovoljile sve te zahtjeve one mogu koristiti postojeće alate poput normi ISO 9001, ISO 14001, ISO 27001 i drugih. Integracijom više ISO normi u jedan integrirani sustav moguće je zadovoljiti širi spektar zahtjeva. U radu je analizirana mogućnost integracije ISO 9001:2008 sustava upravljanja kvalitetom sa ISO 27001:2010 sustavom upravljanja informacijskom sigurnošću te mogućnosti primjene tog integriranog sustava u praksi. Organizacija sa implementiranim sustavom upravljanja kvalitetom dokazuje da je njen sustav upravljanja kvalitetom sukladan zahtjevima iz norme ISO 9001:2008. Samim time rizik neizvjesnosti vezane uz kvalitetu proizvoda ili pružene usluge za kupce je smanjen, stoga organizacije sve češće teže dobivanju tog certifikata. Kako je u nekim organizacijama potrebna ne samo kvaliteta proizvoda i usluga nego i sigurnost istih, norma ISO 9001:2008 je odličan početak organizacije za primjenu drugih ISO normi, u ovom slučaju norme ISO 27001:2010. Svrha norme ISO 27001:2010 je da pokaže korisnicima da je informacijska sigurnost u organizaciji provedena na najbolji mogući način i da stekne njihovo povjerenje. Stoga možemo reći da norma ISO 27001:2010 znači za informacijsku sigurnost isto ono što ISO 9001:2008 znači za sustav upravljanja kvalitetom. U radu će biti prikazano kako se norme implementiraju pojedinačno te postoji li mogućnost integracije tih normi.*

***Ključne riječi**: ISO 9001, ISO 27001, integrirani sustavi, informacijska sigurnost, upravljanje kvalitetom*

## 1. Introduction

This paper deals with the subject of integration possibilities of quality management system ISO 9001:2008 and Information Security Management System ISO 27001:2010. Organization implemented quality management system proves that its quality management system complies with the requirements of ISO 9001:2008.As some organizations require not only quality of products and services, but also the safety of these, ISO 9001:2008 is a great start for the application of other ISO standards, in this case, ISO 27001:2010. The purpose of ISO 27001:2010 is to show customers that information security in the organization is implemented in the best possible way and gain their trust. Therefore we can say that the ISO 27001:2010 means for information security the same thing as ISO 9001:2008 means for quality management system. In this paper will be shown how to implement the standards individually and whether there is the possibility of integrating these standards.

## 2. Quality management systems

### 2.1. Choice between alternatives

Each organization applies certain quality management system, it is its characteristic. Organizations and owners are aware of the fact that to a greater or lesser extent, they can not survive on the market if they do not have customers for products and services. The degree of quality management is drastically different from organization to organization which is caused by differences that exist among market conditions, size of organization, type of ownership, social culture, management style, business, etc.The quality management system built according to ISO[116] 9000, is the starting point, but over time the requirements of this system are becoming inadequate and need to be supplemented and upgraded to some of the more sophisticated systems.

### 2.2. ISO 9001 standard

Organization with a focus on customers through leadership, teamwork, process approach, systems approach to management, continuous improvement, decision-making based on facts makes standard ISO 9001 the most extensive international standard that sets requirements for the establishment, maintenance of quality management systems and is applicable to organizations of all types. ISO 9001 covers the basic processes within the organization, it also provides certain actions for control over processes and management that is controlled. Quality Management System according to ISO 9001 standard is now used throughout the world and gaining certification of the system proves the quality of products or services, that's why the ISO 9001 is generally accepted.

## 3. Implementation of ISO 9001:2008 standard

### 3.1. Advantages that the ISO 9001 standard brings to organisations

Particularly important for the safety of products and services is the process of acquiring that must be driven by the requirements of ISO 9001:2008 standard, which increases the preventive safety of products and services.ISO 9001:2008 standard is an excellent foundation for the application of other ISO standards in the field of management.It is primarily intended for the construction of a quality management system, which is for the information security the  ISO / IEC 27001[117] standard.

### 3.2. Implementation (introduction and establishment) of quality management system ISO 9001:2008

For the introduction of quality management system according to ISO 9001:2008 and certification of system, depending on the size of the organization or institution, the diversity of processes and products or services, an average of 2-12 months is needed. The establishment of quality management system and certification takes place according to certain phases, such as preparatory activities that include recording and analysis of the current situation (organization, resources, processes), good education of management personnel and key employees for the introduction of quality management, planning activities needed to establish the quality management system.

### 3.3. Certification of quality management system ISO 9001:2008

By obtaining the certification of the ISO 9001:2008 standard, certificate of conformity is provided of business with an internationally recognized standard, greater confidence of business partners and customers, a good marketing promotion,  an objective and independent external evaluation and assessment of quality management system.

## 4. Information security management system

### 4.1. Information system protection

„Risk of Information/Internet technology is a danger that its application leads to undesirable consequences (damage) in an organizational system and/or its surroundings. Abuse mostly occurs

[116] ISO is the international organization for standardization (ISO – International Standards Organization)

[117] ISO 27001 is an international standard that defines the requirements of the Information Security Management System for organizations

due to two reasons, namely to achieve unjustified or unlawful use by individuals or organized groups or for applying material or non-material damage to the individual, group or community. The most vulnerable are the information systems that can access the Internet, because the Internet in itself is extremely compromised"(Klasić, Klarić 2009:160).

Part of the activity that is related to the application of information technology in the business world was supposed to be planning information system protection therefore ISO organization has organized the subcommission number 27 upon which standards for information system security are made. Therefore, the establishment of organizational control and protection management of information systems is the purpose of the standard ISO/IEC 27000.These standards give recommendations and the necessary elements (with respect to the specifics of each system) that should be followed in the preparation of their own security management model and standards for establishing, implementing, maintaining and improving information security management system.

### 4.2. ISO 27001:2010 standard

ISO 27001:2010 standard forms the basis of information security, it specifies in which way can any type of organization (profit or non-profit, large or small, public or private) organize information security. The purpose of the ISO 27001:2010 is to show how to introduce information security in an organization, it gives an organization the ability to obtain certification, which serves as a confirmation that the security of an organization is implemented in the best possible way. ISO 27001:2010 means for information security the same thing that ISO 9001:2008 means for the quality management system. The importance of this standard is shown by many jurisdictions that took this standard as a basis for writing a variety of regulations in the area of personal data protection, protection of privacy, protection of information systems, etc.

### 4.3. Advantages of the ISO 27001 standard

The establishment and operation of an ISMS will not, by itself, necessarily reduce the negative risk of information security immediately. In essence, the ISMS is a tool that allows an organization to systematically control the level of information security and performance. The system should provide economic benefits such as reducing the time to research safety, reducing the time to learn new things, reduce disputes, reduce legal fees, possible reduction in insurance premiums, the protection of information assets, increase awareness of information security, increasing the trust with customers and other interested parties. ISO 27001 standard helps to protect the confidentiality of information in a way that keeps them accessible only to authorized personnel, standard preserves the integrity, accuracy and completeness of the information, and the availability of information to authorized entities and the possibility of using them. A management system that has been introduced to an organization for the protection of information.

## 5. Implementation, maintenance, monitoring and verification of information security

### 5.1. Implementation

For an organization to receive a certificate of information security management organization must meet a set of requirements defined by the standard ISO 27001. Basic steps in the implementation of ISO 27001 are the beginning of the project, defining ISMS, risk assessment, risk management, training, pre-audit, audit and continuous improvement.

### 5.2. Maintenance, monitoring and verification

Management should regularly carry out verifications of the ISMS to ensure that the scope continues to be appropriate and that there are identified improvements in the ISMS processes. Supplement security plans by taking into account the results of tests and examinations of ISMS. Record the actions and events that could have an impact on the efficiency and performance of ISMS. In order to facilitate supervision and control of ISMS organization must make certain actions. Organization must monitor and review procedures and other controls to timely detect errors, identify successful and unsuccessful attempts at security violations and incidents, in order to determine whether the activities assigned to the staff are appropriate and that the implemented security controls are functioning as expected. It is necessary to detect security events and prevent security incidents.

## 6. Possibilities of integration of ISO 9001:2008 and ISO 27001:2010 standards

„In the organization where the management decides to integrate the management system, it is necessary to identify the area of different systems that integrate. It is necessary to identify those areas, processes, standards or requirements that are fully integrated into a single form and that the requirements in an integrated form remain independent"(www.kvaliteta.net).

As there is an increasing need for an integrated management system, every year there is an increasing number of organizations that implement such a management system in their organization. Various systems are being combined and one of the possible ways of integration is that of a quality management system and information security management system. „The most important principle, which leads to the introduction and integration of such systems of management is the principle of gain. Some are direct, others are indirect, where the results are shown in a certain period of time."(www.kvaliteta.net).

Although it seems that the two standards are entirely different, but a more detailed study shows many similarities. One of the similarities is that they have the same four mandatory procedures such as internal audit, document management, corrective actions and preventive measures. Therefore, if the organization requires implementation of both standards, ISO 27001 will be easier to implement because by taking over the elements of ISO 9001, ISO 27001 will be much faster to implement.

## 7. Conclusion

The ISO 9001 standard is the most widely used international standard and is applicable to all organizations, all of which has been achieved with its approach within the organization, through obtaining certification of the system organization is proving the quality of products or services. ISO 9001 covers the basic processes within the organization, it also provides certain actions control over processes and management that is controlled.The quality management system enables an increase in profit due to better sales results, cost reduction of inadequate products, provides us with competitiveness and a better market position, making business reputation.The main reason for the introduction of ISO 9001:2008 in the organization is to achieve stability of the organization and to satisfy the needs all interested parties.We can also say that the ISO 9001 standard is the basic standard which can be upgraded to any other standard, in this case it is ISO 27001:2010. We can say that it is necessary to establish a safety management system if this is of direct relevance to the success and continued operation of the organization. An important factor in recognizing the organization as a reliable and modern business partners is implemented information security system because it represents the implementation of the necessary measures to achieve a satisfactory level of information security within the organization.Advantages of norms are stressed if they are applied over the course of the project implementation of information security and durring the planning of activities. Management system that was introduced in the organization for the protection of information, and complies with ISO 27001 provides an efficient instrument to verify the effectiveness of information security management system. The goal of this standard is the maximum protection of information systems and business resources.

Integration of quality management system ISO 9001:2008 and Information Security Management System ISO 27001:2010 is possible and desirable to all organizations that seek quality of its products and services and information security.

## REFERENCES

IsecT Ltd (2007): ISO27k implementers' forum, www.ISO27001security.com

Klasić, K., Klarić, K.(2009): Informacijski sustavi. Zagreb: Intus informatika

Knez, J. (2006): Sigurnost informacija po normi ISO/IEC 27001 u postojećim sustavima upravljanja,http://issuu.com/kvaliteta.net/docs/knez_j_rad?viewMode= magazine& mode=embed (17.08.2012.)

Lazibat, T. (2009): Upravljanje kvalitetom. Zagreb: Znanstvena knjiga

Norma ISO 9001:2008. ISO, 2008

Norma ISO 27001:2010. ISO, 2010

Oslić, I. (2009):Normom preventivno povećavamo sigurnost proizvoda i usluga, http://www.manager.hr/naslovnica/item/normom-iso-90012008-preventivno-povecavamo-sigurnost-proizvoda-i-usluga (20.08.2012.)

Skoko, H. (2000): Upravljanje kvalitetom. Zagreb:Sinergija d.o.o.

IsecT Ltd.(2007): ISO27k implementers' forum, www.ISO27001security.com

www.kvaliteta.net, (accessed 20 Januar 2013)

www.top-consult-grupa.hr, (accessed 22 Januar 2013)