ADOPTION OF STANDARD FOR INFORMATION SECURITY ISO/IEC 27001 IN BOSNIA AND HERZEGOVINA

Anis Skopak
International Burch University
Bosnia and Herzegovina
anis.skopak@gmail.com

Semir Sakanovic
International Burch University
Bosnia and Herzegovina
symorgh13@gmail.com

Abstract: *When it comes to security, no company in the world can be too cautious. Many companies own and use different systems for protection of data and information from intentional or non-intentional loss, unauthorized access, or abuse. However, the legal aspects of information security systems are well known in order for system to be internationally accepted and adopted. Because of this, the standard ISO/IEC 27001, which ensures positioning in relation to competition through marketing usage of this certificate, fulfills all requirements of the client for information security; reducing the risks associated with information relevant for the organization, reducing operating costs for the prevention of complaints and other incidents, and optimization of the process because the tasks in the organization are clearly defined and understood. ISO/IEC 27001 process of certification is carried out by a certification body that is accredited by schemes that are under the supervision of the IAF (International Accreditation Forum), as only these certificates are a guarantee of global standard acceptance. This study has examined the surveys of twenty (20) large companies, whose scope guarantees the suitability to this standard, and explored the way of implementation, and more importantly that the certification companies in Bosnia and Herzegovina offer this feature. In the end we compared the results of this study with the results from the region and the world.*

Keywords: ISO/IEC 27001, International organization for standardization, Information security management system, ISO, ISMS

Introduction

History of this certificate dates from 1995 when United Kingdom Government's Department of Trade and Industry (DTI) wrote BS7799 standard in several parts. First part of this standard contained Information Security Management which was adopted by International Organization for Standardization as ISO/IEC 17799, "Information Technology – Code of Practice for Information Security Management" in 2000. The International Organization for Standardization (ISO) is an international standard setting body composed of representatives from various national standards organizations. Founded in 1947, the organization promotes worldwide proprietary, industrial and commercial standards. It is headquartered in Geneva, Switzerland, and as of 2013 works in 164 countries (Secupent). In 2007, ISO/IEC 17799 is renamed for the last time into ISO/IEC 27002. The second part of the BS7799 standard, which was presented in 1999 as "Information Security Management Systems – Specification with Guidance for Use", was focused on implementation of Information Security Management System (ISMS).

In 2005, together with the third part of BS7799 standard it became ISO/IEC 27001:2005 standard. His successor was the advanced version of ISO / IEC 27001: 2013. In the area of security of information resources currently applied increasing number of standards adopted so far, and some standards are still in the process of drafting and adoption procedure should go to their implementation could begin. ISO / IEC 27000: 2009 - Information technology - Security techniques, represents a standard that provides an overview and introduction to the family ISO27 standards, as well as the dictionary of specific terms used in ISO27 vocabulary. ISO / IEC 27001: 2005 - Information Security Management Systems Requirements, (Ex standard BS 7799-2). Is the basic standard for the establishment, implementation, control, promotion and certification of information security (ISMS - Information Security Management System). ISO / IEC 27002: 2005 - Code of Practice for Information Security Management, (former ISO / IEC 17799). Standardizes the Guidelines for the implementation of recommended protection measures (control) and provides an overview of best practices to protect information resources. ISO / IEC 27003: 2010 - ISMS Implementation Guide, represents the standard that provides guidelines for successful implementation of ISMS in accordance with ISO / IEC 27001. ISO / IEC 27004: 2009 - Information Security Management Measurement, represents the standard that gives guidelines to carry out measurements in order to assessment of effectiveness of the ISMS. ISO / IEC 27005: 2008 - Information security risk management, represents standard which provides guidelines for risk management, information security and implementation of the system of information security based on risk management. SO / IEC 27006: 2007 - Guide to the certification / registration process, represents the standard that specifies requirements for the accreditation of certification bodies - ISMS according to ISO / IEC 27001 requirements, outlines the specific requirements for certification and together with ISO / IEC 17021 is a basic standard accreditation. ISO / IEC 27011: 2008 - Information technology - Security techniques, represents the standard that provides guidelines for telecommunications organizations implement recommended protection measures ISMS (also known as ITU X.1051 as standard). ISO / IEC 27033 - IT network security, represents the standard security IT networks, was introduced as a replacement for multitask standard based on ISO / IEC 18028: 2006 specification (this standard was adopted in part). ISO 27799: 2008 - Health informatics, represents the standard that provides guidance for ISMS implementation in the health sector.

ISO/IEC 27001

Lately, more and more attention is paid to the dangers that are closely related to the protection of data in companies. The issue of data protection applies to all types of businesses, regardless of their status, size or area of operations and activities. The best and absolutely need a system to solve the problem of information security, including loss or theft, the information security management system "Information Security Management System - ISMS '', which includes the availability, integrity and determination of the degree of confidentiality of information. The method, which allows solving the problems information security, has been developed and is described in ISO-IEC / BSI internationally recognized standards ISO 17799 / ISO 27001 certification of management systems built on the basis of these standards company confirms its commitment to the protection of data according to applicable laws in the industry and legal requirements, enabling a significant instrument competitiveness in the market. the construction of ISMS is particularly important for companies that use internal and / or external computer systems with stored sensitive information, for companies whose business processes are dependent on information systems, and to all other companies that simply want to adapt to the requirements of information security. This is especially true for organizations such as banks, IT companies, financial institutions and insurance companies, hospitals, schools, universities, car manufacturers, call centers, tax offices, consulting firms and many other companies.

ISO 27001 is an international standard published by the International Organization for Standardization (ISO) and describes how to manage information security companies. The latest version of this standard was published in 2013, and the current full name is ISO / IEC 27001: 2013. The first revision of the standard was published in 2005 and was developed based on the British standard BS 7799-2. ISO 27001 can be implemented in any organization, profit or non-profit, private or public, large or small. They wrote him the world's best experts in the field of information security and prescribe the methodology for the application of information security management in an organization. Also, enables companies to obtain certification, which means that the independent certification body provides certification that the organization has implemented information security in accordance with ISO 27001. ISO 27001 has become the most popular standard of information security in the world, and many companies are certified to him.

International Standard ISO / IEC 27001: 2005 prescribes certain set of requirements for the establishment of systems for information security management (Eng. ISMS - Information Security Management System). Proper fulfillment of these requirements, i.e. their implementation, the organization created a holistic environment in which risks to information timely observed, in order to eliminate or reduce the same. With the establishment of the management system, the organization is able to continuously monitor and review all aspects of information security, and to make the necessary and effective improvements. As a result, we have continuous improvement of the security situation. Standard ISO 27001 i.e. The system for managing information security that derives from it, is applicable to banking and financial institutions, IT industry, economic sector, all public or private organizations.

ISO 27001 is focused on protecting the confidentiality, integrity and availability of data in the company. This is achieved by recognizing that potential problems can happen to the data (i.e., risk assessment), and the definition of what should be taken to prevent such problems (i.e. The treatment or processing risk). Thus, the basic philosophy of ISO 27001 is based on risk management: identifying and systematic analysis of risks. Safety measures to be implemented are usually in the form of policies, procedures and technical applications (i.e.. Software and equipment). However, in most cases, companies already have all the necessary hardware and software, or use them in an insecure manner - thus most applications ISO 27001 relates to the establishment of organizational regulations (i.e. Write documents) that are necessary to prevent security breaches. Given that such applications require multiple management policies, procedures, people, resources, etc., ISO describes how to fit all these elements in the information security management system (ISMS). Therefore, the information security management is not only about IT security (i.e. Firewall, protection against computer viruses and so on.) But also on process management, legal protection, human resources management, physical protection and the like. ISO 27001 is aligned with other management systems, and supports the implementation of integrated with other management system standards.

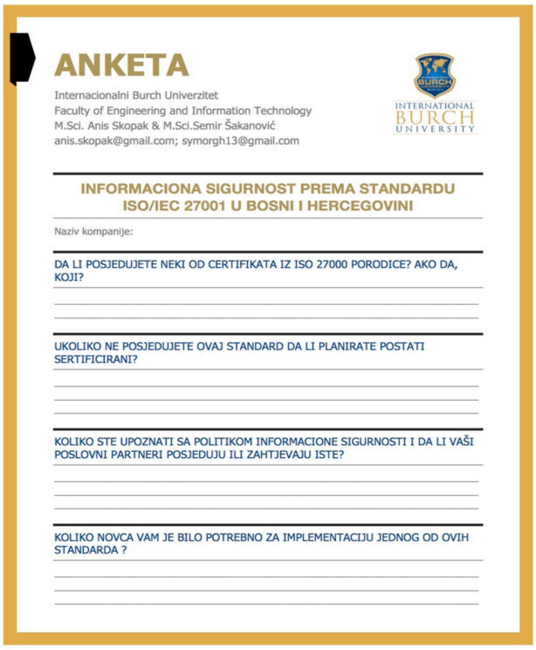
ISO 27001 is harmonized with the management system standards such as ISO 9001 and ISO 14001, ISO 27001 focuses on a continuous improvement process information security management system, contains requirements relating to documentation and records, including risk assessment and management processes using PDCA (Plan, Do, Check, Act) model. Norma comprehensive approach to security information. Different assets / assets owned organizations require protection. Some of them are digital information, the information in paper form, physical resources such as computers and networks, the knowledge that the organization has. The account must be taken wide degree areas of competence development of staff to the physical / technical security. ISO 27001 will help you protect your information according to the following principles: Confidentiality ensures that information is accessible only to people with authorized access, integrity monitor and ensure the accuracy and integrity of information and methods of management information, availability ensures that the authorized personnel have access to the necessary information and adequate resources. There are two types of ISO 27001 certification: (a) for the organization and (b) for individuals. Organizations may be certified in order to demonstrate compliance with all mandatory clauses standards; Individuals can take the course and pass an exam to get a certificate. To be certified as an organization, you must implement the standard as outlined in the previous sections and then pass a certification audit by the certification body. The certification audit was carried out through the following steps: Phase 1 (Document Review) - auditors will review all documentation, Phase 2 (main audit) - auditors to perform the audit on the spot to verify whether all activities of the company in compliance with ISO 27001 and documentation system information security management Supervisory visits - after certification, during the validity period of three years, auditors will verify whether the company maintains information security management system.

To implement ISO 27001 in the company, you have to follow these 16 steps:

1. Provide support of top management
2. Use project management methodology
3. Define the scope of information security management system
4. Write roof privacy policy
5. Define risk assessment
6. Conduct risk assessment and treatment
7. Write seventh Statement of applicability
8. Write the Risk Treatment Plan
9. Define ways of measuring the effectiveness of security measures and information security management system
10. Implement all applicable safety measures and procedures
11. Implement training programs and awareness
12. Carry out all daily activities prescribed documentation of your information security management system
13. Track and measure your information security management system
14. Establishment of internal audit
15. Conduct Management Review
16. Implement corrective measures

Sixteen rules for the implementation of ISO 27001

ISO/IEC 27001 standard in Bosna and Herzegovina



ANKETA

Internacionalni Burch Univerzitet
Faculty of Engineering and Information Technology
M.Sci. Anis Skopak & M.Sci.Semir Šakanović
anis.skopak@gmail.com; symorgh13@gmail.com

INTERNATIONAL BURCH UNIVERSITY

INFORMACIONA SIGURNOST PREMA STANDARDU ISO/IEC 27001 U BOSNI I HERCEGOVINI

Naziv kompanije:

DA LI POSJEDUJETE NEKI OD CERTIFIKATA IZ ISO 27000 PORODICE? AKO DA, KOJI?

UKOLIKO NE POSJEDUJETE OVAJ STANDARD DA LI PLANIRATE POSTATI SERTIFICIRANI?

KOLIKO STE UPOZNATI SA POLITIKOM INFORMACIONE SIGURNOSTI I DA LI VAŠI POSLOVNI PARTNERI POSJEDUJU ILI ZAHTJEVAJU ISTE?

KOLIKO NOVCA VAM JE BILO POTREBNO ZA IMPLEMENTACIJU JEDNOG OD OVIH STANDARDA ?

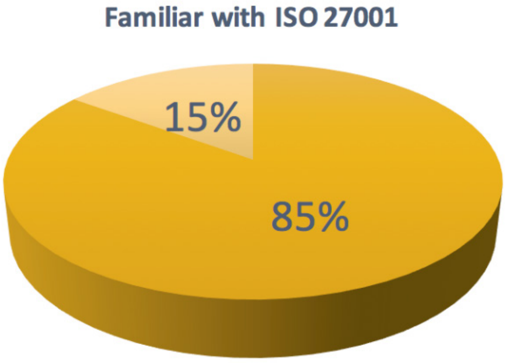
Survey

The world now has about 200 countries (193 UN member states). Average one country has about 8,000 certificates. There is a legitimate question where is Bosnia and Herzegovina, and its economy and other entities. According to the latest data available to the Foreign Trade Chamber of Bosnia and Herzegovina currently has about 1,400 certificates. Of these, ISO 9001 represented over 90%, while certificates of ISO 14001 and OHSAS 18001, as well as key in the environmental management and health and safety at work, minor represented. The competent national authorities should pay more attention to and care for the faster adoption of EU directives and harmonization of our legislation. You should also provide continuous and procedural simple financial support to companies for the preparation and implementation of individual certificates. In the future, as we get closer to EU membership, all the greater will be the need for certification, to manufacturing and service firms. One should be careful to time, as in some similar situations, not to be slaves to the system "give what you give, because after this." Practice shows that in a well-organized company with well-organized and consultations required several months of intensive work, but for more complex processes and more than one year to obtain a certificate. This should confirm that the BH. businesses introduced new standards that apply to selective European and world markets, and not only that owns the paper, which is not a rare case. Also, in the world there is a trend that is increasingly companies which have two or more standards in the application. Companies are introducing an integrated system consisting of a base of ISO 9001, ISO 14001 and BS OHSAS 18001 or ISO 9001, ISO 14001, HACCP or ISO 9001, ISO 14001 and FSC CoC, etc. What is encouraging is that some of our companies that had a single certificate follow this practice, and more of those who have two or more of the standard.

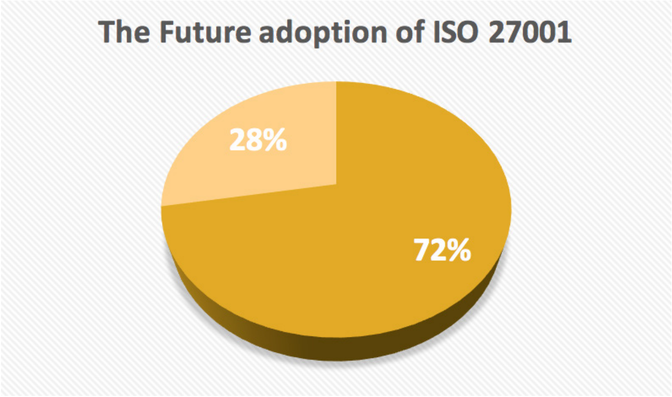
In this research (M.Sci. Anis Skopak and M.Sci Semir Šakanović), we did the research followed a survey that we submitted to the addresses of twenty companies in Bosnia and Herzegovina, looking for answers whether companies in Bosnia and Herzegovina have implemented ISO / IEC 27001 certified, and if they do not have to I have basic knowledge regarding the benefits or the implementation thereof. It should be noted that we check our results with the list of certified organizations in BiH by the standards of the Foreign Trade Chamber of Bosnia and Herzegovina, and that we get the information when it is made from certified companies to implement standard working on the introduction of standards.

Results

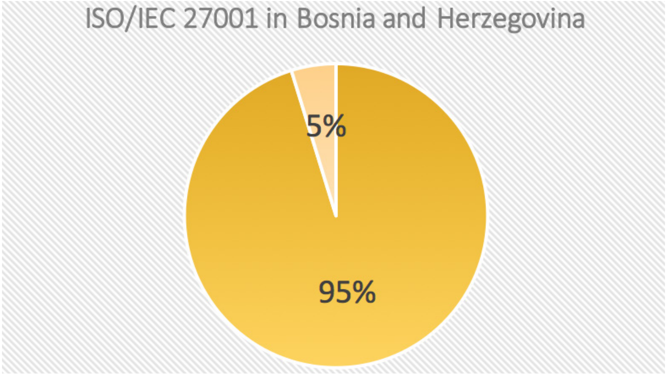
In this research, we found that 85% of our citizens are familiar with this certificate, and also to know the way of its procedures and that they already had contact with the introduction of other ISO standards in their companies.



What is particularly interesting is that our respondents mostly aware of the benefits of this standard, and its primary benefit is improvement in the status of the company. Awareness of European integration and international business objective is to all of the companies surveyed, the Administration ISO certifications are confirmation of the quality of services offered. Thus, 72% of our respondents said that they are considering in the future to adopt the implementation of this system, as well as some others.



But when we look at companies that have already implemented this system, the situation is not at all promising. Even 95% of the company does not have implemented ISO 27001, although considered to be useful. Given that we have in our survey included some of the largest companies in Bosnia and Herzegovina set us question what is the general number of companies that have ISO 27001 certification?



From the Foreign Trade Chamber of Bosnia and Herzegovina have been given information on the leading companies for certification in Bosnia and Herzegovina, which are certainly the most prominent TUV SUD Sava d.o.o, SGS d.o.o., Det Norske Veritas. So we created this list of companies among the thousands of companies in Bosnia and Herzegovina only possess ISO 27001. Among the certified companies in Bosnia and Herzegovina now are: Sarajevo International Airport, the Lottery of Bosnia and Herzegovina, Partner MCF, CS Computer Systems, Institute for Commercial Engineering, ComTrade, KING ICT and several banks and micro-credit organizations.

Number of certified companies in Bosnia and Herzegovina barely exceeds the number 10, which is quite small compared with the number of registered companies in this country. When we considered state of the Western Balkans, Croatia 36 organizations has been certified ISO / IEC 27001, Serbia 15, while Macedonia 3 in other countries there is no ISO 27001 organizations. Among other countries, the largest number of certificated organizations are in Japan (3657).

Organizations can themselves specify the scope of ISO / IEC 27001 certification in accordance with their own wishes and possibilities. The scope of the implementation of standards and statements of applicability of the standards should be harmonized, and that the documents are crucial in the process of certification. If an organization wants sertificirati one of its organizational units, then this certificate does not apply to other entities, and those in this case does not have to be certification and are not subject to revision. Certification is completely is voluntary act of an organization, but in modern business is increasingly the subjects of our suppliers and business partners to possession of a certificate in information security. An independent assessment of information security and its periodic ravizija bring organizations quite strict and formalized and implementation, which requires prior approval of management. Possession of a certificate of information security indicates the potential of the organization in terms of fed up information resources and to upgrade the status of secure and credible business partner.

Conclusion

It can be concluded that the information security policy is a document that allows the organization of the establishment of security over the entire information resources. Development of a comprehensive program for the protection of information resources should enable the protection of people and information, set rules of behavior of all users of information resources defines a consequence of safety rules and minimize risk, and constant monitoring of compliance with legislation. As there are already a number of standards in the field of information resources, it is necessary to systematically approach the process of their evaluation and certification. Accordingly, we can conclude that the certification process needs to start adopting ISO / IEC 27001 as the basic standard for the establishment, implementation, control, promotion and certification of information security (ISMS - Information Security Management System), from which it should subsequent to certification of specific basin, information resources at a higher level. ISO / IEC 27001, in order to establish a comprehensive system of protection of information resources, determines the system for the protection of information, the responsibility of executives, determining the procedures of internal control systems to protect information, ATMI procedures validation system for the protection of information, and procedures related to improving the system for the protection of information.

When it comes to the adoption of the above standards in Bosnia and Herzegovina, it can be concluded that the current situation is quite unfavorable in relation to the country's developed regions in the world, considering that only a few organizations have adopted ISO / IEC 27001.

Reference

Hajdarević K, Infrasturctures Proactive Information Security Metrics for Computer Network Architectures and, based on ISO 27001, Internacionalnni Burch Univerzitet, Sarajevo, 2013.

Vanjskotrgovniska Komora Bosne i Hercegovine,
http://komorabih.ba/wpcontent/uploads/2013/05/Baza_certificiranih_organizacija_BiH_apr_2015.pdf

Diver S., Information Security Policy - A Development Guide for Large and Small Companies, SANS Institute, Bethesda, Maryland, 2007.

International Organization for Standardization, ISO/IEC 27000, Geneva, 2009.

Petrović R. S., Čekerevac Z., Milanović Z., Međunarodna naučna konferencija Menadžment 2010, Politika informacione bezbednosti kao element prevencije kriznih situacija, Srbija, Kruševac, 2010.

About the ISO27k Standards, http://www.iso27001security.com/html/iso27000.html, 2010.

About the ISO27k Standards, http://www.iso27001security.com/html/27001.html, 2010.

Danchev D., "Building and Implementing a Successful information Security Policy." 2003., http://www.windowsecurity.com/pages/security-policy.pdf

International Register of ISMS Certificates, http://www.iso27001certificates.com/Register%20Search.htm, 2010.

ISO - International Organization for Standardization, http://www.iso.org/

NERDA, ISO/IEC 27001, http://www.nerda.ba/pdf/standardi/ISO-IEC%2027001.pdf