[1.]Lilja ŠIKMAN, [2.]Tihomir LATINOVIĆ, [3.]Darko PASPALJ

ISO 27001 – INFORMATION SYSTEMS SECURITY, DEVELOPMENT, TRENDS, TECHNICAL AND ECONOMIC CHALLENGES

[1.]University of Banja Luka, Faculty of Technology, Banja Luka, BOSNIA & HERZEGOVINA
[2.]University of Banja Luka, Faculty of Mechanical Engineering, Banja Luka, BOSNIA & HERZEGOVINA
[3.]University of Banja Luka, Faculty of Safety Science, Banja Luka, BOSNIA & HERZEGOVINA

Abstract: Businesses, government and public institutions have long been facing a great challenge. The use of modern information technology in business requires the introduction of integrated measures for the protection of information. Recommendations and the use of the international standard ISO / IEC 27001 enabled the successful planning and implementation of systems for information security management. Great importance at this standard is given the concept of information resources/assets. Information is also an information resource and every information resource have its value. If there is a disturbance value of information resources deals with the attacks and security threats to these resources. Security threat represents any event that results in a distortion of the basic requirements of security: confidentiality, integrity and availability of information. Therefore, implement physical, technical and administrative safeguards. If it happens some of the attacks on information resources it hinders the business and reputation of businesses. Modern methodology of information protection includes a risk assessment. It is therefore necessary before establishing a system of security to determine the optimal level of safety in terms of cost-effectiveness in terms of costs and speed implementation of the necessary security measures. Too large range of security systems and over-planned level of security that can impede the establishment of system security and higher costs compared to a profit of implemented security measures. In this study we explored the dynamics taking place use and application of standards to date. The distribution and implementation of standards by industrial areas.

Keywords: information security, ISO 27001

1. INTRODUCTION

If we want to achieve information security must be taken of the activities that imply legislation, policy security, business functions, organizational structure, and the commitment of management to introduce and invest in a system for managing information security - Information Security Management System (ISMS). Legislation in the organization provides a number of important activities related to the protection of information, personal data, reports and respect for intellectual property rights. With the rapid development of information technology, businesses are faced with new and different risks for the security of information resources.

To achieve the appropriate level of information protection requires effective implementation of ISMS. When the leadership of an organization chooses to implement and the introduction of the ISMS, it means that they are committed to the process that makes the information safe and to has accepted the availability of appropriate resources to support the processes in the organization that will provide safety information. The consequence of such a decision management team related to the processes related to the management system, educational workshops and increase user awareness of the system of protection of information. Special stage in the implementation of ISMS is the process of managing security risk, which determines the selection of security controls that should provide transformation to a system for managing changes in the business in a safe environment.

The standard is important for all institutions whose business functions related in any way with information technology and the demand for the protection of confidentiality of information resources. Applying this standard provides better connections with close organizations in the wider environment. The introduction of this standard, businesses show their customers and all interested parties that their business functions implemented on the basis of the principles of security and that the business plans are focused on continuous improvement of the system for information security management.

2. DEVELOPMENT OF INFORMATION SECURITY

In the late 60s and early 70s of last century began the development of security policy information in a modern form, which is recognizable today. During this period, security policy info existed only within parts of classified information the government sector, defined internal security procedures and protected from the public. Over the next ten years, each secret and public information-space through the prism of globalization and democratic processes is transformed into transparent areas of data. These areas are still important in terms of the requirements of security of information. This data area is characterized by modern information space, which is: unclassified information, classified information, personal data in a broader sense the intellectual property, the concept of electronic government administration (Klaic, A., 2006).

Security procedures for implementing the policy of information security vary per property protection. The analysis of the traditional approach to security policy information in the public sector is classified information facility protection, and established a model of protection is applied to technology, processes and people, in whose framework is made sharing of such information. The modern sense of security policy information within the business sector as an object of protection means of information resources in a broad sense (Institute for Standardization of Serbia, 2014).

The concept of information security in BiH is defined by law and is dealt with in a way that is today accepted in developed countries and ensuring compatibility with the concept of information security of the European Union. The term information security means a condition in which the secured integrity of hardware, processes and data, their availability and confidentiality of data and information. It should be borne in mind that information security is not the same thing as IT security. Specifically, information security refers to the protection of information regardless of the medium on which it is stored and transmitted. System information security includes natural persons and environment, processes, organization and technology (Official Gazette, 2017). Safety information in a wider sense is not related to the safety and protection of information resources, namely: people, service,

3. ISO / IEC 27001

Standard ISO / IEC 27001 with formally accepted as' 'Information technology - Security techniques - systems for information security management - Requirements' (Information Technology -Security Techniques - Information Security Management Systems - Requirements) was released in October 2005 as a replacement for British standard BS7799-2. The standard lists specific requirements which are important when establishing, implementing, monitoring, reviewing, maintaining and improving information security management system. It is aimed at the safety requirements of general character and does not consider the specific safety requirements for the organization of the same type and can be applied to businesses of various types and sizes. Standard is a document that defines the rules, guidelines or characteristics for activities or their results in order to achieve the optimal level of regulation (Ministry of Information Society of Montenegro, 2009). Bearing in mind that the standard sets out what needs to be done to make the system more secure it is possible to single out three aspects of information security:

Table 1. Overview of the basic aspects of security in ISO / IEC 27001

Basic aspects of security information defined in ISO / IEC 27001	Which contain requirements
Information	Defining and analysing the characteristics of IT equipment, the rules of access to information, passwords, encryption procedures, policies from the point of occurrence of risk to the security of data and information, instructions for handling media, e-commerce services, relationships with suppliers, network security management, maintenance and development.
Technically	Control physical access, protection workspace, video monitoring, recording and control of employees.
Organizing	Security policy, organization of information security, managing information resources, security, human resources, operational procedures and responsibilities, management of security incidents, management business.

Analysing the requirements in the table above, the standard defines a general framework for establishing ISMS with the basic concept to provide complete protection of information. Bearing in mind that it can be applied to different types and sizes of businesses, recommended as a model of safety information for different types of applications, and including the following benefits (Pleskonjić et al, 2007):

- The formulation of requirements and goals of security,
- Provides efficient management of security risks,
- Respect of formal laws and regulations,
- The framework for the management and control processes for the implementation, in order to meet individual security goals of the institution,
- Management of protection in the definition of new processes,
- When identifying and clarifying the existing procedure of information security management,
- Management in institutions can use it to determine the status of activities relating to information security management;
- For an appointment of the level of compliance with regulations, procedures and standards in the organization when assessing by internal and external auditors,
- As proof of all other organizations and business partners that this is an institution that has a strategic goal - implementation of protection of information resources, etc.

4. CONCEPTUAL FRAMEWORK OF ISMS APPLICATION

ISMS is important for any branch of industry and for the private and public business sectors. This standard is provided confidence in the safety and security of the necessary information. For the successful implementation of the most important initiatives of the leadership and support for the introduction of the ISMS, and the willingness to overcome all possible problems that can occur at the same time. When the leadership of the organization decided to introduce ISMS, then consciously assume responsibility for procedures such as ensuring the availability of all essential resources for the operation of the ISMS, appropriate training of all employees covered by the ISMS, as well as competence development and awareness security. Establish the ISMS is a decision that belongs to the area of strategic planning of the organization and it is in accordance with the business functions and requirements of the organization. The introduction of the ISMS in an organization depends on the goals and needs of the organization, security requirements, business processes, structure and size of the organization. Design ISMS aims to constantly improve operations, and activities that provide such a goal are risk management information security, surveillance, records of security incidents, review of the efficiency and performance of the ISMS. The following table shows a conceptual model that includes procedures and stages of establishing ISMS into organizations.

Table 2. Conceptual framework of establishing ISMS in organizations

ISO / IEC 27001- proposal procedures	The implementation phase
The definition of policy areas and ISMS	1-Identification of business goals 2-Consent and support management 3-A sample of the art application
Assessing security risks risk management Selection of security measures to be introduced Preparing the SOA document	4-Selection of risk assessment methods 5-Identifying information resources based on risk assessment 6-Risk management - risk assessment, a plan to reduce and maintain an acceptable level of risk 7-Selection procedures for risk control 8-Training of employees
Methods review and IA certification	9-Establishment of ISMS 10-Preparation for certification
Enhancing and improving ISMS	11-Procedures repeating periodic audits, risk assessments and continuous improvement

5. INFORMATION SECURITY POLICY

Privacy Safety Information (PSI) is a document that aims to develop a comprehensive plan for the protection of information resources. The implementation of the PSI and reduces the likelihood of power data, the rapid development of information technologies appears new threats to information systems. Therefore, once established policy should regularly analyse, modify and update it whenever the need arises (Ministry of Information Society of Montenegro, 2009).

The rules are defined in the PSI in the organization include hardware and software, the responsible person related to the operation of information systems, employees, users of the system and the people who have the right to access, outside associates. The management organization defines the necessary requirements for information security in the context of security policy. PSI defined standard is based to give three basic safety requirements, which are: confidentiality, integrity and availability of information. In addition to meeting the basic requirements of security and the role of responsibility for security in the organization PSI contains the following:

- authentication - for Internet connection, network access, remote access
- access control and authorization
- physical security - protection of computer equipment, environmental facilities, rooms with servers
- how to manage incidents and respond to incidents

Through the implementation of PSI employees in the organization are converted to the participants in the efforts of organizations to implement information security, where it helps reduce the risk of potential security breaches from errors caused by human factors. When creating a safety policy shall be provided assistance in the definition of critical Information resources organizations and how to protect them (Danchev, 2014).

The responsibility of employees to information security should be defined in the contract. The employees in the organization must work according adopted guidelines and recommendations and consequently behave as well as sanctions in case of security incidents. Treaty pointing in same regulated procedures regarding rules of conduct during the entry, modification or termination of employment.

6. TECHNICAL AND ECONOMIC CATEGORY application of standards

In recent years the ISI / IEC 27001 has undergone an extensive application and there has been its spread throughout the world. For information security standard is recognized as best practice and most organizations seeking to be certified as thus gain a competitive edge within their markets. Leading industrial sectors according to the number of ISO / IEC 27001 certificates are presented in the following figure 1 (ISO Survey, 2018).

The greatest application of standards in the world has an organization in the field of information technology. The reason is that in electronic business information with qualitative properties of capital and thus have the same importance as financial capital. For this reason, and information security more complex. Therefore, during the development and implementation of the ISMS, and the process of preparation for certification ISO / IEC 27001 real help for organizations regardless of size, type and nature of the business.

Modern trends of development are characterized by the globalization of markets and plans for standardization in the field of information security so that is imposed on the need and obligation to our environment and implement actions towards the implementation and improvement of system security information. In Bosnia and Herzegovina is a growing number of organizations that have implemented the standard ISO / IEC 27001, which is viewed in Figure 2 (ISO Survey, 2018).

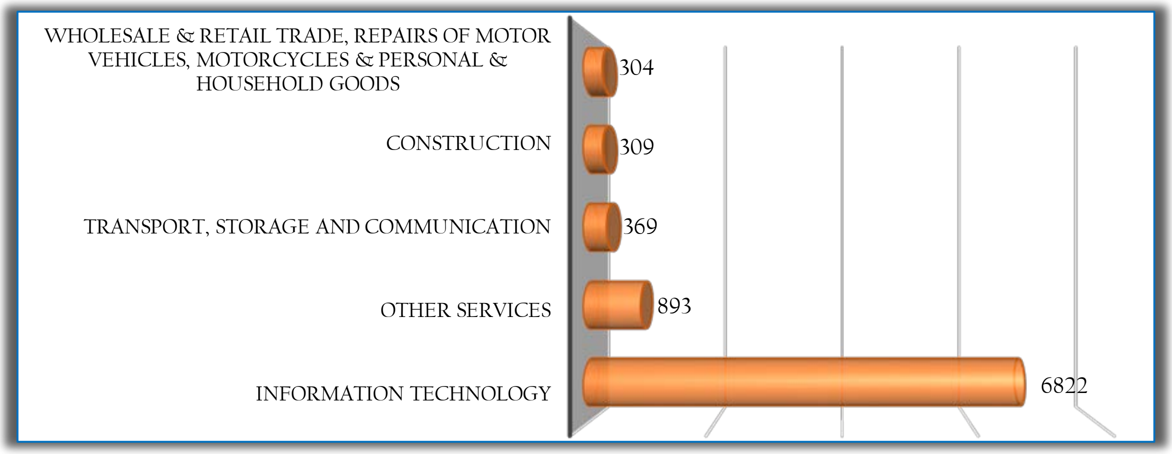

Figure 1. Standard ISO/IEC 27001 - the highest number of certificates per sectors in the world in 2018

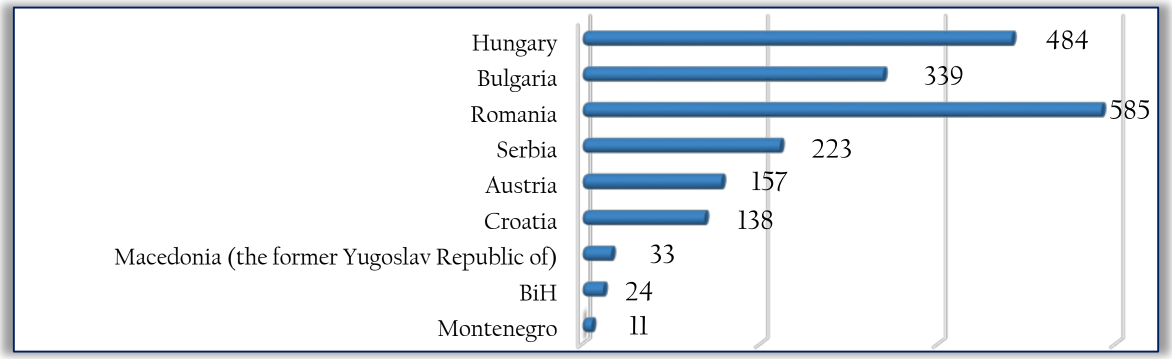

Figure 2. Standard ISO/IEC 27001- number of certificates - number of certificates in surrounding countries in 2018

The certification and the implementation of the standards organizations have numerous economic and technical advantages, some of which are:

- ensuring confidence in clients,
- Risk Management provides risk reduction in business activities,
- improving the business environment,
- improving the security and availability of information flow.

Every organization aims to maintain a competitive advantage in the market. To achieve that, organizations tend to fulfil and sustain the needs of its users. Some of the internal benefits of successful ISMS implementation in organizations are:

- raising awareness of employees,
- Operational efficiency is improved (the responsibility of employees, etc.)
- mutual communication between employees and the organization is better,
- the better and safer operation, and enhanced protection of information resources,
- better quality products and services.

7. CONCLUSIONS

Every organization has to target the security business, which provides protection business of information resources. Therefore, the introduction of ISMS represents the application of the necessary procedures for the provision of appropriate levels of security within informatics organizations. In this way organizations become recognizable as modern and reliable business entities that security challenges facing the system and react in time. This business commitment has resulted in achieving better market position of businesses.

References

[1] Danchev, D., (2014). Building and Implementing a Successful Information Security Policy, http://www.windowsecurity.com/pages/security-policy.pdf
[2] The Institute for Standardization of Serbia (2014). ISO / IEC 27001: 2014, ISO / IEC 27002: 2015
[3] ISO Survey 2018 Downloads 19.10.2019. https://www.iso.org/the-iso-survey.html
[4] Klaic, A. (2006). Information Security Requirements and the Information Systems Planning Process, .17th IIS Conference. (P. 265-269). Varaždin: FOI
[5] Ministry of Information Society of Montenegro. (2009). Privacy of information security in Montenegro. Podgorica
[6] Pleskonjić, M., N. Macek, Djordjevic, B., Carić, M. (2007). Security of computer networks and systems, Micro books, Belgrade
[7] Official Gazette, (2017), Decision on the adoption of policies to manage information security in the institutions of Bosnia and Herzegovina, for the period 2017 - 2022. https://www.mkt.gov.ba/dokumenti/informatizacija/ostali_propisi