ISMS ACCORDING TO STANDARD ISO/IEC 27001

ISMS PREMA STANDARDU ISO/IEC 27001

Džemal Kulašin*
Faruk Unkić**

ABSTRACT

Recent manifestations of cyber crime as a ransomware, where an immense number of computers all over the world has been encrypted, additionally indicate (un) expected weaknesses of information security even with branding business systems. This intensified the significance of organizational approach to information security and the necessity of establishing adequate system of managing the protection of both digital and typical information. That system is known as Information Security Management System (ISMS).
For establishing this type of system, certain bases are needed, and the best ones are those ISO/IEC 27001international standard requirements. This paperwork is about the basics of Information Security Management System (ISMS) with ISO/IEC 27001 standard bases whereas the focus is on the implementation of ISMS according to "the best practice" standard and benefits that a successful implementation would provide.

Keywords: Information security, Information Security Management System, ISO/IEC 27001

SAŽETAK

Poslednje manifestacije cyber kriminala u formi ransomware-a gdje je nepovratno enkriptiran ogroman broj računara u gotovo svim zemljama svijeta, dodatno je ukazao na (ne)očekivane slabosti informacijske sigurnosti, čak kada su u pitanju i renomirani poslovni sistemi. Time je dodatno osnažen značaj organizacijskog pristupa informacijskoj sigurnosti, odnosno nužnost uspostavljanja odgovarajućeg sistema upravljanja posvećenog isključivo zaštiti informacija, bilo u digitalnom, bilo u klasičnom obliku.Takav sistem poznat je pod imenom Sistem upravljanja informacijskom sigurnošću, odnosno Information Security Management System (akronim ISMS).
Naravno, za uspostavljanje ovakvog sistema potrebne su odgovarajuće podloge, a najkvalitetnijim se smatraju zahtjevi međunarodnog standarda ISO/IEC 27001. U ovom radu, predstavljaju se osnove Sistema upravljanja informacijskom sigurnošću upravo na podlogama standarda ISO/IEC 27001, gdje je akcenat na implementaciji ISMS-a prema standardu "najbolje prakse" te benefitima koje uspješna implementacija donosi.

Ključne riječi: Sigurnost informacija, Sistem upravljanja sigurnošću informacija, ISO/IEC 27001

INTRODUCTION

The importance and complexity of preserving information security in the circumstances of the technological turbulent environment forces the organization to the regulatory system of information security, where the solution of the so-called " Information Security Management System - ISMS (Information Security Management System). This concept is a systematic approach to information security management in organizations that includes processes, employees, an IT system, and a security policy that ensures the preservation of key aspects of information security known as

* - Fakultet za menadžment i poslovnu ekonomiju Univerziteta u Travniku
** - Ekonomski fakultet Univerziteta u Zenici

the C-I-A security confidentiality (Integrity-Availability).[1]

Information security, by this approach, is achieved by the application of appropriate controls (ie security measures) relating to security policies, business processes, procedures, organizational structure, and function of hardware and software. All of these controls need to be designed, implemented, monitored, reviewed and improved to ensure the fulfillment of business and safety requirements. Obviously, an appropriate basis for the establishment of an information security management system is needed, where the ISO / IEC 27001 standard is considered to be of the highest quality.

International Standard ISO / IEC 27001[2] specifies requirements for the establishment, application, maintenance, and continuous improvement of information security management systems in the context of the organization. "What is very important, it is also emphasized that" ... the set requirements are general and intended for use in all organizations, regardless of their type, size or shape.[3] However, the practice so far shows that the ISO / IEC 27001 standard is the most represented in the sectors of technology, finance, the business services sector, governmental bodies at the state or local level and telecommunications, while other sectors account for only 8% of the certificate of this standard[4].

STRUCTURE STANDARD ISO 27001

The ISO 27001 standard is distinguished by the comprehensiveness of the structure, whereby we distinguish: (1) the information aspect, where the performance of IT equipment, access rights, encryption, passwords, protocols, policies from the aspect of data security risk and information are analyzed and defined, (2) aspect, where clear instructions, policies and procedures for generating information, their distribution, storage and (3) physical aspects, where physical access control, employee records, video surveillance, workstation protection, etc. are defined. Accordingly, the ISO 27001 standard covers not only the security of the IT domain, as it is often wrong interpreted but also covers "... physical and technical protection, human resources, relationships with suppliers, partners and clients, legal and regulatory obligations, business continuity etc."[5]

The standard is structured in 11 chapters and Annex A, where the first three chapters are introductory, while the remaining chapters are mandatory, and the requirements in these chapters must be implemented in an organization that establishes ISMS on the basis of this standard. In doing so, it is noticeable that chapters are named as in other management systems (eg ISO 9001: 2015), which facilitates their mutual integration, which is in accordance with the ISO / IEC Annex of the International Organization for Standardization. The ISO 27001 standard chapters are as follows[6]:

0: Introduction. Explains the purpose of ISO 27001 and its compatibility with other management standards.

1: Scope. Specifies the general requirements of ISMS applicable in different types of organizations.

2: Normative references. References to ISO / IEC 27000 as a standard essential for the establishment of ISMS. The rest of the ISO27k is optional.

3: Terms and definitions. References to ISO / IEC 27000 where the necessary terms and

1 Acronym C-I-A I: Confidentiality or secrecy (Confidentiality), integritet or completeness (Integrity) and availability or availability informacija (Availability)

2 U Would standard It also carries a national prefix, and it marks as: Low ISO/IEC 27001:2015

3 Institute for STANDARDIZACIJIn BiH, official web site: http://www.bas.gov.ba/pages/page_1369.html [27.05.2017]

4 https://www.itgovernance.co.uk/download/ISO27001-Global-Report-2016.pdf [31.05.2017]

5 http://www.consalta.ba/en/Sistemi-upravljanja/isms-iso-27001[02.06.2017]

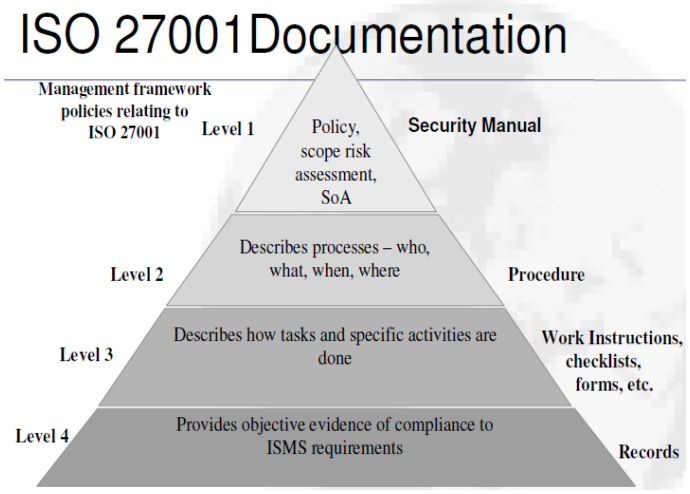
6 http://www.iso27001security.com/html/27001.html [29.05.2017]

definitions are given.
4: Context of the organization. It specifies the organizational context, needs and expectations of "stakeholders", and defines the scope of ISMS.
5: Leadership. Specifies that the top management must demonstrate leadership and commitment to ISMS, define security policy, determine roles and responsibilities.
6: Planning. Defines the conditions for risk assessment, risk management, statement of applicability (SoA), risk management plan with clarification of information security objectives.
7: Support. Defines the conditions for the availability of resources, competencies, information, communication and control of documents and records.
8: Operation. Defines models for risk assessment and risk management, as well as security measures and other processes needed to achieve data security.
9: Performance evaluation. Defines the conditions for monitoring, measurement, analysis, assessment, internal audit and management review.
10: Improvements. Defines the conditions for compliance, corrections, corrective measures and permanent improvements to ISMS.

However, it is interesting that the crucial part of the ISO 27001 standard is, in fact, Annex A, because it contains a wide set of security controls that need to be applied in order to protect information [6]. The security controls of Annex A (in particular, 114 controls) are arranged in 14 sections, as follows[7]:
A.5. Information security policies - 2 controls
A.6. Organization of information security - 7 controls
A.7. Human Resources Security - 6 controls
A.8. Asset Management - 10 controls
A.9. Access control - 14 controls
A.10. Cryptography - 2 controls
A.11. Physical and Environmental Security - 15 controls
A.12. Operational security - 14 controls
A.13. Communications security - 7 controls
A.14. System acquisition, development and maintenance - 13 controls
A.15. Supplier relationships - 5 controls
A.16. Information security incident management - 7 controls
A.17. Aspects of information security aspects of business continuity management - 4 controls
A.18. Compliance - 8 controls

As can be seen, some sections of Annex A have different number of security controls, and according to their number, we see the "severity" of a particular security section represented in ISMS according to ISO 27001. Of course, in every organization, all the security measures provided for in this The Annex, because their choice depends on the results of the risk assessment as one of the steps in the establishment of ISMS.
Certainly, within the structure of ISMS according to ISO 27001, in particular, its documentation should be emphasized, which is more pronounced in relation to other management systems. Globally, ISMS according to the ISO 27001 standard consists of a series of documents, which is at the top of the Safety Policy Rules or Security Manual (Level 1), Procedures (Level 2), Work Instructions (Level 3) and Records (Level 4) (Figure 1).

Picture 1: ISMS documentation levels according to ISO 27001



7 https://advisera.com/27001academy/what-is-iso-27001/ [28.05.2017]

IMPLEMENTATION OF ISMS-A ACCORDING TO ISO 27001

The ISO 27001 standard focuses on protecting the confidentiality, integrity and availability of data in an organization (C-IA). This is achieved by identifying potential problems that can occur with data, i.e. risk assessment, and defining what should be done to prevent such problems, i.e. risk management. Therefore, the basic ISMS philosophy implemented according to ISO 27001 is based on risk management. Based on risk assessments, and in accordance with the objective of implementing the ISO 27001 system, the necessary controls are ensured in order to protect information and data from "stakeholders"; The interested parties to whom this management system is addressed can be clients, organizations and companies, employees, associates, but also the society in a wider sense. In other words, the framework ISO 27001 includes Risk Assessment and Treatment and the implementation of Safeguard Implementation.

As implementation of ISMS according to ISO 27001 standard is a complex, long-term and continuous process, it must be implemented in steps, according to a certain order. Key steps in implementing ISMS according to the ISO 27001 standard can be the following:

1. Decision on the establishment of the ISMS
2. A record of the state of information security,
3. Appointment of the ISMS team
4. Team education,
5. The scope and boundaries of the introduction of the system,
6. Information security policy,
7. Property inventory and valuation,
8. Risk assessment
9. Risk management and implementation of planned controls
10. Creating documentation
11. Educating employees and raising awareness of information (non) security.

The actual implementation of ISMS in an organization is, in essence, the implementation of security controls selected according to the risk assessment carried out on the basis of the organization's security policy. Otherwise, the document in which this is stated and officially signed is designated as a statement of applicability (SoA - Statement of Applicability), as strictly stated in the requirement of ISO 27001. Thus, if the risk assessment is of good quality, and what is it is planned, it is possible to expect well-established ISMS in which the planned level of CIA is achieved. On the other hand, if the risk assessment is poorly or partially made (for example, only in the part of the property of the information system), it is certain that no matter how well planned security measures are implemented, the established ISMS is not good.

PDCA CYCLE IN ISMS

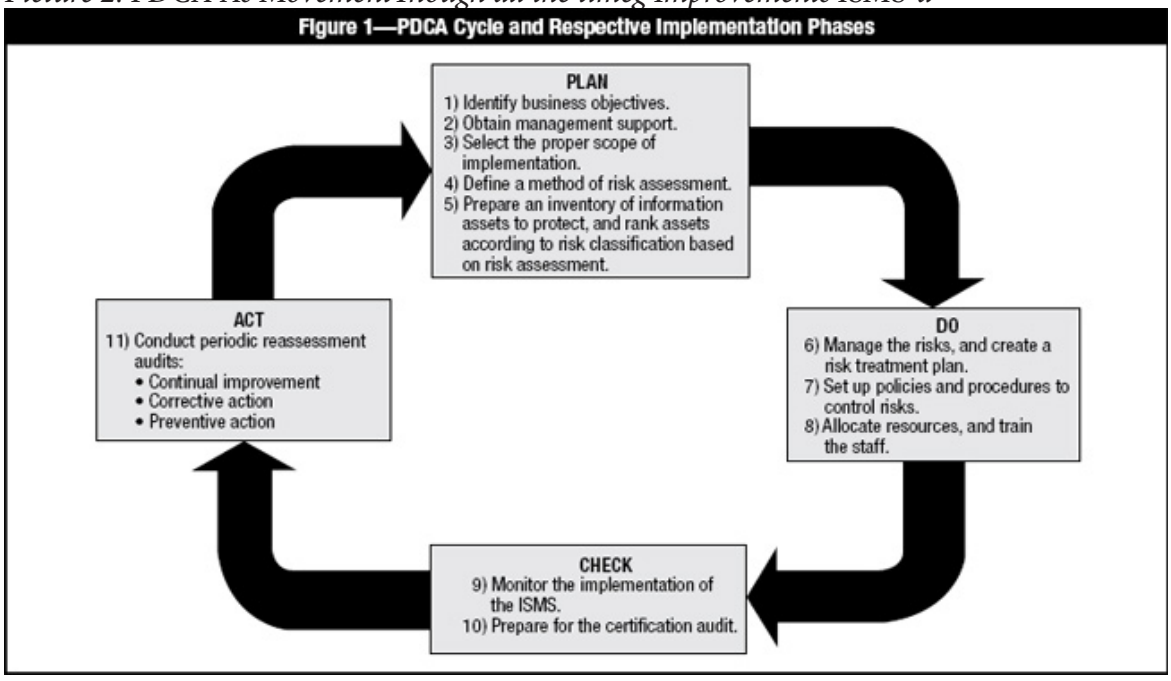
Quality and successful ISMS according to the ISO / IEC 27001 standard is also characterized by the so-called. PDCA cycle (Plan-Do-Check-Action), which is otherwise happening in all ISO-based management systems based on a series of continuous improvement engines. For ISMS, which covers the area of Information and Communication Technology (ICT), such an approach is necessary because of the speed of technological changes and frequent security incidents initiated both from within and outside the system. The closer the meaning of the particular phases of the PDCA cycle in this context is the following:

– Planning (Plan): The policy of the information security management system, together with the goals of the information security management system and the defined measures to improve the system in terms of improving information security, make "Plan-Plan" a part of the information security management system in accordance with the requirements of ISO 27001. Based on the user's stated requirements and through the establishment of the policy of the ISMS organization, it enters

the phase of establishing or planning an information security management system (ISO 27001). At this stage, activities are also being carried out to define the criteria for risk assessment, the approach and the methodology for risk assessment are defined, the levels of risk acceptability are defined, and so on.

– Implementation (Do): Implementation of planned actions on the application of previously selected control mechanisms and objectives, development, implementation and implementation of risk reduction plan, awareness training on ISMS implementation, ISMS resource management, etc. Structure and responsibility, training, competence and awareness, documentation and control of documents, control of operations and preparedness for emergency response and response to them make "Do-Do" part of the information security management system in accordance with the requirements of ISO 27001.
– Checking (Check): This phase is the ISMS review based on defined procedures for reviewing, measuring the effectiveness of control mechanisms, conducting internal checks, updating risk reduction plans, etc. The part of the "Check-Check" of the information security management system in accordance with the requirements of the ISO 27001 standard consists of monitoring and measuring, evaluating compliance, corrective and preventive actions, records management and internal system checks.
– Improvement (Action): This part of the information security management system in accordance with the requirements of ISO 27001 is achieved through a review by management that rounds the whole cycle of performance of the management system and returns it to the planning (Plan) that should result in continuous improvement. As the final phase in this continuous improvement cycle, the ISMS maintenance and improvement phase is being implemented through the introduction of improvements, the taking of corrective and preventive measures, checking that the improvements implemented are sustainable.

Picture 2: PDCA As MovementThough all the timeg Improvements ISMS-a



[Source: https://www.kvalis.com/implementacija-isms-prema-isoiec-270012013/]

The PDCA cycle can also be seen in individual chapters (ie requirements) of the ISO 27001 standard[8]:

- Chapter 4. Context of the organization 5. Management and 6. Planning are part of the PDCA Phase Planning,
- Chapter 8. Operation is part of the PDCA Phase Implementation,
- Chapter 9. Effectiveness is part of the PDCA Phase Check
- Chapter 10. Improvements are part of the PDCA Phase Improvement.

BENEFITS OF ISMS ACCORDING TO THE ISO 27001 STANDARD

The ISO / IEC 27000 series of standards provides a harmonized approach to risk management that exposes information values in the organization through the development, implementation and maintenance of ISMS as an information security management system. With its ultimate certification, the organization acquires both internal and external advantages, such as:

-1. creating trust in the organization's information system,

- Complementarity with the legal regulations related to information flows because it is a standard that has clear flexibility,

-3. focusing on clear continuous improvement of processes that provide information security, increasing preventive action through reduction of "bottlenecks" in the network,

- 4. reduction of incidents and better understanding of causes,

- 5. Generally develop employee awareness in terms of the importance of information protection[9], Etc.

The effects of implementing ISMS are often the topic of various research in the world, where all indicators affirmatively speak about the benefits of the established information security management system. One of these research is the benefits divided by individual sectors of the organization, such as management, finance, sales and marketing and the IT sector (Picture 3).

However, according to the official data of the International Organization for Standardization (ISO), which publishes once a year an overview of ISO certificates, in our country there is no necessary level of corporate awareness in this respect. Namely, according to the latest ISO Survey[10], end of December 2015 in Bosnia and Herzegovina, only 13 certificates were issued for the established ISMS according to the ISO 27001 standard[11]. For comparison, it is worth mentioning data from the same source that far more certificates were issued in neighboring countries: in Slovenia 58 certificates, in Croatia 96, while in Serbia 103 certificates were issued.

CONCLUSION

Organizing a management system dedicated solely to protecting information, i.e. the Information Security Management System (ISMS) is becoming more and more important because the increasingly difficult and diverse forms of cybercrime are manifested every day throughout the world. Dramatic financial losses, which are expressed at hundreds of billions of dollars (??) On an annual level, are often conditioned by (internal) human factors, failure to perform regular backups, obscurity in the implementation of hardware and software updates, and so on. With the successful implementation of the Information Security Management

8 Koutic, D, 2014, Has the PDCA Cycle been removed from the new ISO standards, advisor, available at: https://advisera.com/27001academy/blog/2014/04/13/has-the-pdca-cycle-been-removed-from-the-new-iso-standards/[30.05.2017]

9 https://chapters.theiia.org/ bermuda/ Events/ Chapter Documents/ Information %20Security%20 Management%20System%20%28ISMS%29%20Overview.pdf [29.05.2017]

10 http://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1 [29.05.2017]

11 BAS ISO/IEC 27001 were acquired by: central Bank BOsne I Hercegovine, lottery BOsne I Hercegovine, BH Telekom, Institute for Economic Engineering Zenica, etc.

Picture 3: Effects of implementation of ISMS according to ISO 27001

System (ISMS) on the ISO / IEC 27001 standards, security risks are reduced to the projected acceptable level, as the complex organizational system for secrecy, integrity and data availability (C-I-A) is harmonized. According to the experience of numerous world companies, the ISO / IEC 27001 certification certifies numerous advantages, both internal and external, which ultimately not only maximizes the level of security protection, but also improves overall organizational efficiency. However, the ISMS Implementation Project is a complex and demanding project, which has its origins in a clear and firm commitment to top management, and then on continuous intellectual and infrastructural efforts to improve the existing system.

REFERENCES

[1] ACCVIS ISO 27001, 2015, Sistem menadžmenta zaštite i bezbednosti informacija, dostupno na: http://accvis.com/iso-27001-2015-iec/ [Pristup: 27.05.2017]

[2] Adelsberger, Z. 2015, Implementacija ISMS prema ISO /IEC 27001/2013, ICT Security Kladovo, 14.-16.maj 2015, dostupno na: http://www.slideshare.net/dejanjeremich/adelsberger-zdenko-implementacija-iso27001-2013 [Pristup: 30.05.2017]

[3] Hofer, D., 2014, Implementacija sustava upravljanja informacijskom sigurnošću prema ISO 27001:2013 - Koraci i prednosti, STEP Osiguranje kvalitet Zagreb, dostupno na: https://issuu.com/kvaliteta.net/docs/hdk_14_konferencija_2014.157-163 [Pristup: 28.05.2017]

[4] Košutić, D, 2014, Has the PDCA Cycle been removed from the new ISO standards, Advisera, dostupno na: https://advisera.com/27001academy/blog/2014/04/13/has-the-pdca-cycle-been-removed-from-the-new-iso-standards/ [Pristup: 30.05.2017]

[5] IT Governance, 2016, ISO 27001 Global report - 2016, dostupno na: https://www.itgovernance.co.uk /download/ISO27001-Global-Report-2016.pdf [Pristup: 31.05.2017]
[6] Raković, R., 2013, Sistem bezbednosti informacija - iskustva i preporuke information security system - experiences and recommendations, dostupno na http://www.infotech.org.rs/blog/wp-content/uploads/radovi2013/071.pdf / [Pristup: 26.05.2017]
[7] Terroza, S.K.A, 2015, Information Security Management System - Overview, The institute of internal auditor, dostupno na: https://chapters.theiia.org/ bermuda/Events/Chapter Documents/ Information%20Security%20Management%20System%20%28ISMS%29%20Overview.pdf [Pristup: 29.05.2017]
[8] https://www.kvalis.com/implementacija-isms-prema-isoiec-270012013/ [Pristup: 28.05.2017]
[9] https://advisera.com/27001academy/what-is-iso-27001/ [Pristup: 28.05.2017]
[10] https://www.iso.org/the-iso-survey.html [Pristup: 29.05.2017]
[11] http://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1 [Pristup: 29.05.2017]
[12] http://www.iso27001security.com/html/27001.html [Pristup: 29.05.2017]
[13] http://www.consalta.ba/en/Sistemi-upravljanja/isms-iso-27001[Pristup: 02.06.2017]