Original article

PROJECT OF ISMS IMPLEMENTATION IN ORGANIZATION – ASPECTS AND PRACTICAL EXPERIENCES

Radoslav Raković

Energoprojekt-Entel a.d., Belgrade, Serbia

Received: 14 December 2020
Revised: 12 January 2021
Accepted: 27 April 2021

Abstract: The Information Security Management System (ISMS) represents one of the most complex management systems for implementation in an organization. The comlexity of this system, based on the standard ISO 27001:2013, is a consequence of specific Annex A of the standard that defines 14 areas of information security, with 35 security objectives and 114 controls. Some of these controls are technical, some organizational and some combined ones. It asks the project of ISMS implementation in the organization to be carefully planned and implemented. In this paper, some project management specific aspects related to implementation of this type of project are considered and some practical experiences of the project of ISMS establishment and further improvement in particular organization are presented.

Keywords: Integrated Security Management System, Project Management, Risk Management, Statement of Applicability, General Data Protection Regulation (GDPR).

1. INTRODUCTION

The Integrated Management System (IMS) of an organization, as a rule, consists of three basic management systems – quality (Quality Management System - QMS), environmental protection (Environmental Managament System - EMS) as well as occupational health and safety (QH&S) Management System – defined by particular international standards (ISO, 2015a; ISO, 2015b; ISO,2018a). Additionally, some specific standards can be included, depending on area of business activities of particular organization, as well as its commitment to which segments of IMS will give priority. One of the most common additional management system is the Information Security Management System (ISMS).

The ISMS is probably one of the most complex management systems for implementation in an organization, even for organizations that have experience with establishment of other management systems. This fact is the consequence of specific normative Annex A of the standard ISO 27001 (ISO, 2013) that defines reference control objectives and controls. These controls define in detail elements of the ISMS, technical, organizational as well as combined ones. No any of these controls could be ommitted, only different levels of application should be foreseen. Taking this into account, it is clear that project for establishment of such a standard within the organization should be carefully planned and implemented, as a framework for future development and improvement. In this paper, some project management specific aspects related to implementation of this type of project are considered. Firstly, brief overview of the standard ISO 27001 as well as General Data Protection Regulation (GDPR) is given. Then,

Corresponding author. Email: rrakovic@ep-entel.com
ISSN 2560-4961 (online)

https://doi.org/10.18485/epmj.2021.11.1.3

some specifics of implementation of such type of project are discussed from the point of view of project management aspects. Finally, some case study related to practical experiences of the project of ISMS establishing and its development by harmonization with new revision of standard as well as including of GDPR elements in particular organization are presented.

2. BRIEF OVERVIEW OF ISO 27001

The information security management system (ISMS) standard ISO 27001 defines framework for protection of basic information propreties – confidentiality, integrity and availability (CIA). The standard includes basic information security requirements, related to information security risk assessment and treatment, information security incident management and business continuity management. In comparison with other management standards, the ISO 27001 standard has a separate Annex A, dedicated to specific security controls, aimed at eliminating or reducing the above mentioned risks to an acceptable level.

The first revision of the ISMS standard was issued in 2005 (ISO, 2005). The Annex A of this standard included 133 security controls grouped into 11 areas odf security and 39 security objectives. The actual revision of the standard was issued in 2013 (ISO, 2013) with two main changes – harmonization with Annex SL as well as change odf structure and number of controls within Annex A.

The unified high level structure of all management system standards issued by the International Organization for Standardization (ISO) is defined in the document titled Annex SL (ISO, 2012). As per this structure, each management standard consists of 11 chapters, as follows:

- Chapter 0: Introduction
- Chapter 1: Scope
- Chapter 2: Normative references
- Chapter 3: Terms and Definitions
- Chapter 4: Context of the organization, including external and internal issues and definition of the subject management system as a whole
- Chapter 5: Leadership, including management commitment, policy as well as organizational roles, responsibilities and authorities
- Chapter 6: Planning, including actions to address risks and opportunities, objectives and planning to achieve them
- Chapter 7: Support, including resources, awareness, training, competence, communication and documented information
- Chapter 8: Operation, including opreational planning and control, risk assessment and risk treatment
- Chapter 9: Performance evaluation, including monitoring, measurement, analysis and evaluation, internal audit and management review
- Chapter 10: Improvement, including nonconformity, corrective actions and continual improvement.

The ISO 27001:2013 standard (ISO, 2013) was one of the first management standards harmonized with the subject Annex SL. In the revised standard, the Annex A covers 14 areas of information security, 35 control objectives and 114 security controls. An overview of this Annex is given in Table 1.

Table 1: Information security controls as per Annex A of ISO 27001:2013

	Area of Security	**Number of Objectives**	**Number of Controls**
A5	Information security policy.	1	2
A6	Organization of information security.	2	7
A7	Human resource security.	3	6
A8	Asset management.	3	10
A9	Access control.	4	14
A10	Cryptography.	1	2
A11	Physical and environmental security.	2	15
A12	Operations security.	7	14

A13	Communications security.	2	7
A14	System acquisition, development and maintenance.	3	13
A15	Supplier relationships.	2	5
A16	Information security incident management.	1	7
A17	Information security aspects of business continuity management.	2	4
A18	Compliance.	2	8
	TOTAL.	35	114

The table shows that areas of security cover a wide range of information security issues, each of which is typically focused on either technical or organizational actions, while others combine both of them. Generally speaking, these security areas, including security objectives and specified controls, are global guidelines for holistic approach to information security and represent some kind of reminder for an organization with respect to its main activities. These activities should be implemented to ensure a level of information security adequate to the risk.

The most important document required by the standard is Statement of Appliacability (SoA), as per requirement 6.1.3 d) of the standard (ISO, 2013). This statement summarizes risk treatment actions taken per each control, oriented to achieve acceptable level of information security risks.

Taking this into account above mentioned, it is clear that project for establishment of such a standard within the organization represents very required endeavour that asks full implememtation of project managament approach.

3. PERSONAL DATA PROTECTION - GDPR

The General Data Protection Regulation (GDPR) represents the main document in personal data protection legislative in European Union (EU). This document (GDPR, 2016) was adopted at the end of April 2016, it was put into force in May 2016, and it was applicable as of 25th of May 2018. It consists of preamble with 173 elements defining EU commitment to protect personal data, followed by 99 articles grouped into 11 chapters (some of them have sections). Main purpose of this regulation is to protect rights and freedom of natural persons from EU related to personal data collection and processing, but it is applied also to countries out of EU in situation when in any form process personal data of subjects from EU. This regulation is based on severel principles as lawfull and fair processing, purpose limitation, data minimization, data accuracy, storage time limitation, integrity & confidentiality as well as accountability of controller for processing. The GDPR defines some basic rights of data subject (right to be informed, right for correction, „right to be forgotten“, right to restriction of processing, right to data portability, right to complain, as well as right not to be subject to a decision based solely on automated processing, including profiling), and defines severe penalities for data protection breaches.

Central question is if correctly implemented ISMS as per standard ISO 27001 means full compliance with the GDPR? Unfortunataly, answer is NO (Raković, 2019a; Raković, 2018)! Between standard and regulation there are significant similarities but also some essential differences – regulation is legal document, with mandatory application, standard is voluntary up to decision of an organization to comply with it, or up to its transformation to legal act, because management standard requires organization to be in compliance with laws!

Several important elements in GDPR don't exist in ISO 27001 (Raković, 2019a). The most important is consent for personal data processing (Art. 7&8). Also, similar situation is related to several of data subject rights (Right to erasure i.e. "to be forgotten", Art. 17, Right to restriction of processing, Art 18, Right to data portability, Art. 20, Right to complain, Art 21). International transfer of personal data (Art 46 GDPR) partially exists as approach in ISO 27001, but it is related to business data only.

It is clear that personal data protection is very sensitive topic, with a lot of dilemmas and doubts. It means that process of implementing

GDPR provisions should be carefully planned and realized (Todorović, et al, 2018).

In Serbia was issued new Law on personal data protection (OGRS, 2018), started with application on August 21, 2019. There are several main differences between GDPR and Serbian law (Raković, 2019b):

- Some clauses are defined in different way because Serbia is nor member of EU.
- Serbian Law defines right to objection to Ombudsman, instead of right to complaint. It is known that legal effect of objection and compliant is not the same.
- Penalties in Serbian Law are significantly lower in comparison with those defined within GDPR.

4. PROJECT MANAGEMENT ASPECTS OF THE ISMS ESTABLISHING

Even a brief overview of the standard ISO 27001 and its Annex A with technical, organizational and combined controls illustrate that project of the ISMS establishing is a very required endeavor. Taking into account basic framework related to project management (Jovanović, 2009; Raković, 2011; Raković, 2007) and specifics of the ISMS establishing project (Raković, 2017), following issues should be considered and resolved in adequate way:

- Project objectives. Generally, these objectives include implementation of the ISO 27001 requirements and preparation for certification. In practice, it is usuallly defined measurable and verifiable objective to achieve certification by fixed date at the latest, harmonized with business objectives of the organization.
- Project results. Results of the project implementation are closely related to project objectives and include implementation of all required ISMS processes and obtaining ISO 27001 cerificate.
- Project organization. As a rule, project sponsor of the project is top management of the organization (management representative for IMS, if exists). Project manager should be a person with some level of knowledge and experience in management systems' establishing as well as in IT area. Number and profile of project team members depend on the decision if the organization plans to engage a consultant (typical case) or to implement the ISMS on their own. The project team member should cover both IT and technology of company work related issues.
- Schedule and milestones of the project. As a rule, the ISMS establishing project asks at least 12-18 months. Activities of the project include initiaition, planning, risk assessment and treatment, ISMS documents preparation, ISMS controls' implementation and operation, results review, internal audit, management review, external (certifiaction) audit and continual improvement.
- Tools. For the first, it is necesry to decide which of project management tools will be used (MS Project, Oracle / Primavera, etc) and how the documents produced during the project will be kept (server on local network, etc) to be available for use.
- Reporting. It is necessary to define responsibility and periodicity of the project reporting. As a rule, project manager is responsible person for project progress reports preparation. Regular interval for reporting is usually once a month, optionally at weekly level. In practice, reports are usually prepared weekly and summarized at monthly progress meetings of the project team with the project sponsor.

It is very important to pay attention to two specifics of the ISMS project establishing in comparison with standard projects, mentioned above:

- Continual improvement. It represents one of the basic principles for all management systems, which means that the system is established on some fundamental level and then it is continually improved by enhancing their performances. Practically it

means that the ISMS establishing project can never be completed! Basic part of the project is completed by certification, but in future it continues in form of continual improvement based on experiences in practice as well as findings of regular internal and external audits and management review, in case of new standard revision issuance, etc.

- Risk assessment and treatment. It was mentioned in chapter 2 that controls could be technical, organizational or combined. Independently of its nature, implementation of each control is more or less related to some costs (people engagement, equipment, software, civil and installation works, etc). It means that it is necessary to be very careful, to avoid situation in which investment into control implementation overwhelm benefits achieved. Essentially, Cost / Benefit balance is very important and this is the main reason of risk assessment and tretament significance. Information security risk assessment covers (ISO, 2018c) identifying, quantifying (risk analysis) and prioritizing information security risks against criteria for risk acceptance and objectives relevant to the organization (risk evaluation). Possible options for risk treatment include reducing of risk by implementation of controls, accepting or avoiding risks as well as sharing the associated risks to other parties (insurers, suppliers, etc).

There are 6 basic steps supporting required ISO 27001 risks assessment & treatment (Advisera, 2019):

- Risk assessment methodology. It means determining of rules for performing the risk assessment to ensure the unique approach of all participants in this process, as per requirement 6.1.2 of the standard ISO 27001. These rules cover description how to identify risks causing breach of basic properties of information (CIA), how to identify the risk owners, criteria for assessment likelihood and impact of undesired events, calculation of the risk as well as criteria for accepting risks.
- Risk assessment implementation. Based on above mentioned rules, the potential problems that could arise are identified and determined which ones are unacceptable and have to be treated (identification, analysis and evaluation of the risks). It covers information asset inventory as well as identification of threats and vulnerabilities of the asset to these threats.
- Risk treatment implementation. The main idea is to decrease the risks with minimal investment i.e. to achieve the same result with less money spent. Other options are avoiding the risk (with certain changes in the process), share the risks (transfer to another party) or accepting the risks.
- Risk Assessment Report. It means documenting of everything done in previous steps.
- Statement of Applicability (SoA) preparation. This document summarizes the results of the risk treatment, i.e. describes levels of applicability of all 114 controls.
- Risk Treatment Plan. This document defines exactly who is going to implement each control, in what timeframe, within what budget, etc. It represents practical implementation of the SoA, and includes elements of project management process – resources, time schedule, financial support etc. Without such action plan, the SoA will represent "a dead letter on the paper".

5. CASE STUDY: ENTEL

The main business of the company Energoprojekt Entel p.l.c., Belgrade, Serbia (hereinafter called: ENTEL) is Engineering Design and Consultancy Services related to projects in the fields of Energy, Water, Telecommunications and Environmental protection. Categories of ENTEL's products are design documentation (studies, tenders and technical documents), provision of consultancy services and occasionally customer's specific software development.

The Integrated Management System (IMS) in ENTEL has been established by "step by step" approach. In the first step, in December 2001, the Quality Management System (QMS) as per ISO 9001, was certified by Lloyd's Register Quality Assurance (hereinafter called: LRQA). The establishing of QMS was coordinated by project team consisted of 50% members from the company and 50% members from one consulting company. During the fist two three-years certification cycles emphasis was to consistent performing of quality management system in accordance with specifics of the company, with main idea to establish a basis for expanding the system with other management systems. Establishing of the IMS was started during the third certification cycle, by establishing of Environmental Management System, as per standard ISO 14001:2004 and its certification in the middle of the 2009. Further improvement of the IMS continued at the end of 2010. by establishing of the Occupational Health and Safety Management System, as per BS OHSAS 18001:2007. Certification of this management system originated from activities related to occupational health and safety issues based on legal requirements issued several years ago that created fully new approach, with new responsibilities for both employers and employees. Based on the fact that significant part of its business activities ENTEL carries out within energy sector, it was natural to to establish energy management system as per appropriated management standard. In the first step, ENTEL decided to certify its energy management system as per european standard EM 16001:2009 - system was established during 2010 and certified in the middle of 2011 by LRQA. Meanwhile, new international standard ISO 50001:2011 has been issued and transition to this standard was made in the middle of 2012.

During 2012 ENTEL established Information Security Management System as per the standard ISO 27001:2005 (ISO,2005) and certified it in November 2012 by LRQA. Decision to establish ISMS is based on two main reasons:

- Information protection is very important for organization that works in conditions of market competition
- Information and communication technologies have very important role in ENTEL's activities, with all positive and potentially negative consequences that it may have

We always mentioned in chapter 2 that the standard ISO 27001 is atypical, because consists of basic requirements and additional ones within Annex A of this standard (133 controls, within revision of the standard 2005, reduced to 114 controls within revision of the standard 2013). Except procedures required sa per this standard (IT infrastructure, risk management, incident management, business continuity), it was necessary to prepare and maintain following specific records:

- Registry of information assets. It covers six types of asset – pure information assets (data in diffeernt forms, paper, electronic etc), software asset (applicative and system software), , phisical information asset (computers, servers, local area network, building, rooms, furniture), services (Internet end telecommunication services, electricity, heating, ventilation and air conditioning, fire alarm and fighting systems), human resources (employees, consultants, suppliers, business partners, etc) and non-tangible assets (know-how. licenses, certificates, reputation, etc).
- Risk assessment, based on some risk assessment methodology, taking into account information value of assest (A, from 1, the lowest to 5, the highest), probability of threats (P, from 1, the lowest to 5, the highest) and impact that may have to assets (I, from 1, the lowest to 5, the highest). The most simple methodology is applied – level of risk was calculated as per formula LR = A * P * I, with range from 1 to 100. Level of Risk <25 is acceptable, LR > 75 is un-acceptable, and 25 < LR < 75 asks for some risk treatment actions to be reduces as lower as possible.
- Risk treatment options (acceptance, avoidance, transfer or mittigating risks).

- Statement of applicability (SOA) with overview of implementation of each of 133 (114) controls. Cover page of this document is shown at Figure 1
- Security event / incident report identification and treatment procedure
- Business continuity plan.

ENERGOPROJEKT
ENTEL p.l.c.

STATEMENT OF APPLICABILITY

Clause	Area / Control objective / Control	Status	LR	CR	BR/BP	RRA	Justification of exclusion / Overview of implementation
A.5	**SECURITY POLICY**						
A.5.1	**Information Security Policy**						
A.5.1.1	Information security policy document	⊕			x		Unique IMS Policy has been modified to include elements of ISMS policy and it has been published at ENTEL's site (both Serbian and English) and INFONET
A.5.1.2	Review of information security policy	⊕			x		IMS Policy is reviewed regularly once a year during management review and particular Management Review report is prepared.
A.6	**ORGANIZATION OF INFORMATION SECURITY**						
A.6.1	**Internal Organization**						
A.6.1.1	Management commitment to information security	⊕			x		It is demonstrated through establishing and review of ISMS Policy, defining of responsi-bilities within IMS / ISMS documents and resources assignment - IMS Board, MRIMS, IMS Dept, MIS Dept
A.6.1.2	Information security co-ordination	⊕			x		The ISMS is coordinated by IMS Board, Group for operational support (Team for corrective and preventive actions + MIS representative) and ISIRT Team (MIS Dept + Head of IMS Dept). Within a project, it is responsibility of the Project Manager.
A.6.1.3	Allocation of information security responsibilities	⊕			x		It is implemented through IMS Manual, procedure EN-09P-08 for IT infrastructure and procedures EN-27P-01 to 03. [Working instructions for MIS Dept are available at MISNET, the part of the network visible only for MIS employees (Instructions EN-27I-01, Appendix 1, instructions 3.1 and 5.1.2].

Edition: 1 Form: EN-27P-01F04E Page 1 of 40

Figure 1: ENTEL's SoA, revision 1, 2012

The established ISMS was the subject of internal audit as well as management review, as specific mechanisms of management standards that ensure compliance with the standard and the management system continual improvement.

In this way, ENTEL has been implemented its strategic decision to establish IMS system in accordance with its business activities consisting of quality management, environmetal protection, occupational health and safety, energy management and information security.

Main characteristics and results of the ISMS project establishing were, as follows:

- The project was established as an internal one, but fully in accordance with project management procedure applied to projects ENTEL implements for its external employers (decision on project establishment, Techno-Economic Program of project execution - TEP, representing baseline planning document, deadline for execution, budget, human resources, etc.). The main objective of the project as well as project result was to establish and certify the ISMS in period of 12 months.
- Project was organized on matrix principle, with participants from several relevant organizational units, engaged in parallel at other projects, because ENTEL is a company fully on market and full working hours engagement at the subject project was not possible.
- In spite of ENTEL's experience in implementation of four management systems in previous period, it took really 12 months to finish all activities, from November 2011 to November 2012, as planned.
- The project was implemented on ENTEL's own, except engagement of specialized company to perform limited "penetration" test that

illustrates vulnerability of the local network to breaches form inside and outside. Generally, it was fully in accordance with ENTEL's approach to develop IMS on its own, because of very qualified personnel that covers wide area of activity (more than 70% of employees have university degree). Total engagement was approx. 36 m-m (planned value was 40 m-m).

- Profile of human resources engaged within the project covered the Head of IMS Department (management system specialist, nominated to be project manager), the Management Information System Department (including network administrators, software development specialists, local area network maintenance staff, etc.) and a certain number of project managers (engaged on more complex projects the last few years in ENTEL) with support of the management representative for IMS (Deputy director for projects and marketing) as the project sponsor.
- Project progress was monitored at monthly progress meetings of the project team with the project sponsor, followed by appropriate reports.
- All documents related to the ISMS are available to employees in electronic bulletin board (ENTEL INFONET, segment IMS), together with other IMS documents, Figure 2. The INFONET represents informative site of ENTEL, published at intranet web server.
- The project was successfully finished, within planned time and budget. Decision of ENTEL was to certify the ISMS by the same certification body as for other four management systems. The company certified its ISMS as per ISO 27001: 2005 by LRQA, certificate No BEO0368507/D dated 18 December 2012.

Figure 2: ENTEL INFONET – electronic bulletin board at local network

In October 2013, only one year after ENTEL's ISMS certification, the new revision of the ISMS standard was issued (ISO, 2013). The ENTEL initiated new project to harmonize the ISMS with requirements of the updated standard. As per terminology of management standards, the change of standard revision does not represent continual improvement ("step by step") but radical change ("breakthrough") because improvement "step-by-step" would be last too long. The main activities in this new project were, as follows:

- "Gap analysis" that involved comparison of requirements of the

new revision of standard ISO 27001:2013 vs previous one. As it was mentioned within chapter 2, change of the ISO 27001 was significant, including both change of number and structure of information security controls and harmonization of the standard with unified structure as per Annex SL.
- Transition course for internal auditors to new revision of the standard
- Correction of relevant ISMS documents (procedures, instructions, as well as records, including SoA)
- Implementation of new ISMS in practice
- Internal audit as well as management review.

This project was successfully finished and ENTEL upgraded its certificate to ISO 27001:2013 during LRQA surveillance audit in November 2014. It took 10 months to implement this project and resources spent were at the level of 50% of initial project.

In 2019, ENTEL initiated particular project of the ISMS changes related to implementation of the Law on Personal Data protection (OGRS, 2018), based on GDPR (GDPR, 2016), started with implementation on the 21st of August 2019. The initiation of this project was based on three-year period of monitoring of GDPR implementation in European Union as well as preparation for adoption of the Law in Serbia. The main activities in this new project were, as follows:
- "Gap analysis" that was oriented to identification of main differences between the GDPR and the ISO 27001 standard
- Correction of relevant ISMS documents (particular procedure related to personal data protection, as well as records, including some corrections within SoA)
- Preparation of specific documents related to personal data protection – personal data protection policy, register of personal data, personal data impact assessment as well as personal data risk treatment
- Implementation of changes in practice
- Internal audit as well as management review.

This project was successfully implemented in 2020 and it was verified during the ISMS external surveillance audit in October 2020. It took 12 months to implement the project and resources spent were at the level of 15 m-m.

6. CONCLUSIONS

Previous chapters of this paper illustrate several important things:
- Establishing of ISMS was strategic decision of organization harmonized with its business activities
- In implementation of this decision, approach based on project management was applied
- The ISMS implementation included technical, organizational as well as combined controls based on risk assessment and Cost / Benefit analysis.

It can be concluded that implementation such a complex project is closely related to several management disciplines as strategic management, project management as well as information technology application.

To enable monitoring and measurement of the IMS project results, in 2005. in ENTEL it was established regular poll of employees related to IMS documents knowledge. Each employee had a task to answer five questions (by choosing the correct one among the three proposed) related to contents of IMS documents. The poll, comprising 100 questions, focused on the job carried out by a particular employee, depending on its position within the company. The questions covered all five management standards (QMS, EMS, OH&S, EnMS and ISMS). The first two polls were taken as a corrective action to increase the level of IMS documents knowledge, others were continued as a preventive action after elimination of problems to avert their recurrence.

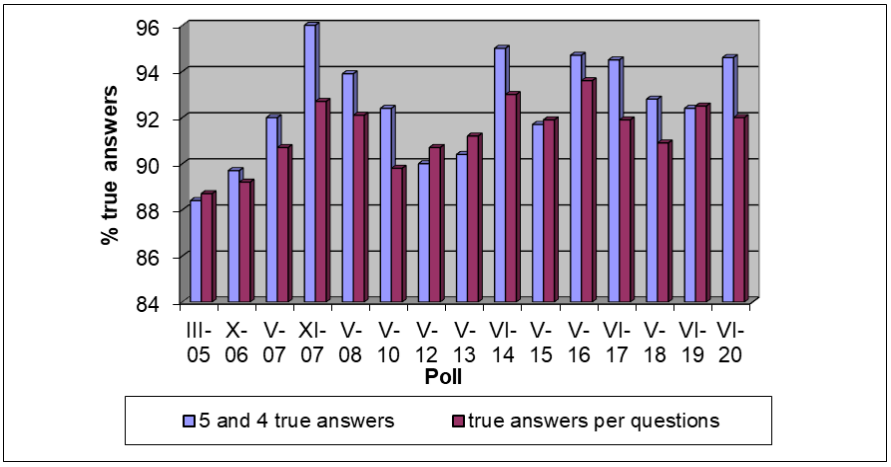

Figure 3: Polling 2005-2020, summary results

The Figure 3 shows summary results of the polling in period 2005 – 2020. It is visible that the number of employees who successfully solved the tasks (5 or 4 true answers) as well as percent of true answers to questions exceed 90%.

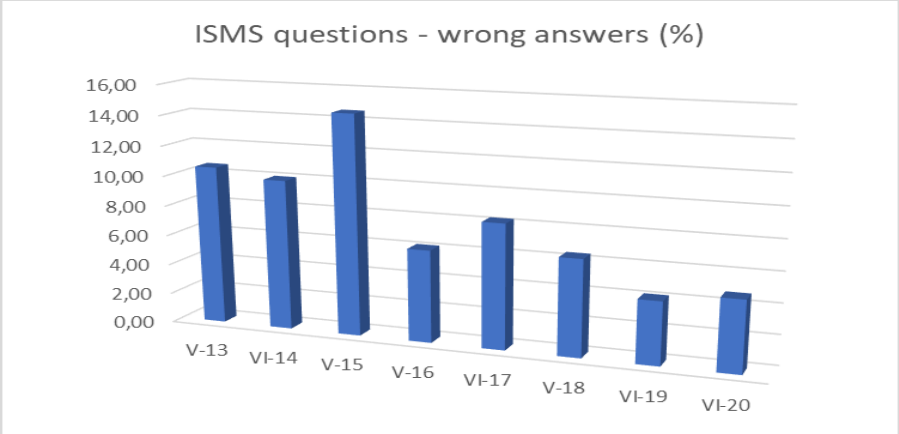

Figure 4: Polling related to ISMS 2013-2020

The figure 4 shows percent of wrong answers related to ISMS from 2013 - 2020. It is visible that after the first few years results are stabilized at the level of 4-8% of wrong answers. Such a high level of ISMS documents knowledge represents guarantee that the ISMS is fully applied in practice.

Implementation of such a complex project confirmed some considerations from the literature (for example, Obradović, et al, 2018) related to project manager's competencies. Technical skills are still significant but to a lesser extent then earlier, conceptual competencies as well as soft skill including decision making and working with people are gaining in importance.

REFERENCES

IMS Documents of ENTEL. (ENTEL, 2012-2020)

ISO 27001:2005 *Information Technology – Security Techniques – Information Security Management Systems – Requirements*

ISO/IEC Directives, Part 1, Consolidated ISO Supplement – *Procedures specific to ISO, Annex SL: Proposals for management system standards, including Appendices 1-3* (2012)

ISO 27001:2013 *Information Technology – Security Techniques – Information Security Management Systems – Requirements*

ISO 9001:2015 *Quality Management Systems – Requirements*

ISO 14001:2015 *Environmental Management Systems – Requirements with guidance for use*

ISO 45001:2018 *Occupational Health & Safety Systems – Requirements with guidance for use*

ISO 50001:2018 *Energy Management Systems – Requirements with guidance for use*

ISO 31001:2018 *Risk Management – Guidelines* (ISO, 2018)

Jovanović, P. (2009). Project Management. Project Management College, Beograd

Law on personal data protection. (2018). Official Gazette of Republic of Serbia. No 87/2018

Obradović, V., Montenegro, A., & Bjelica, D. (2018). Digital Era and Project Management Competencies. *European Project management Journal, 8(1),* pp. 4-9.

Raković, R. (2007). Quality in Project Management – in Serbian. Građevinska knjiga, Beograd

Raković, R. (2011). Project management and quality aspects - principles and practical experiences. *Serbian Project Management Journal, 11(1),* pp. 67-80.

Raković, R. (2017). Information Security - Fundamentals and guidelines – in Serbian. Academic Mind, Beograd

Raković, R. (2018). Personal data protection from the point of view of GDPR regulative. *Kvalitet&Izvrsnost, VII(7-8),* pp. 83-86.

Raković, R. (2019). ISO 27001 vs GDPR – Similarities and Differences. *Kvalitet&Izvrsnost, VIII(1-2),* pp. 39-42.

Raković, R. (2019). Law on personal data protection from the point of view of european lergislative. *Kvalitet&Izvrsnost, VIII(3-4),* pp. 47-52.

Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, Official Journal of the European Union, L 119, May 4, 2016),

Step-by-Step explanation of ISO 27001 risk management (Advisera Expert Solutions Ltd, 2019)

Todorović, I., Komazec, S., Krivokapić, Đ., & Krivokapić, D. (2018). Project Management in the Implementation og General Data Protection Regulation (GDPR). *European Project Management Journal, 8(1),* pp. 55-64.