Turk. J. Math. Comput. Sci.
16(2)(2024) 438–449

DOI : 10.47000/tjmcs.1537584

Impact Analysis and Results of Information Security Management Systems in the Energy Sector

Beyzanur Maden[1,*], Mustafa Alkan[2]

[1]*1Department of Computer Forensics, Informatics Institute, Gazi University, Ankara, Türkiye.*
[2]*Department of Electrical and Electronics Engineering, Faculty of Technology, Gazi University Ankara, Türkiye.*

Received: 13-08-2024 • Accepted: 07-10-2024

Abstract. Strong information security management systems (ISMS) are necessary for maintaining corporate information security. This study was undertaken to examine the viewpoints of professionals in the field of information security within the energy sector and to provide recommendations for system improvements by using the survey method to see the effects of the application of ISMS. A total of 181 participants from the Republic of Türkiye Ministry of Energy and Natural Resources were extensively surveyed. The surveys were grouped as personnel, ISMS employees, and managers. The results were carefully analyzed. It was seen that the personnel in the sector had a largely positive approach to ISMS implementations. The findings obtained in the analysis report were examined in all aspects. Various suggestions for improvements were made for ISMS, especially for increasing awareness training and the number of personnel.

Keywords: Information security, information security management systems, energy sector, critical infrastructure.

1. Introduction

The need for privacy has been one of humanity's most basic needs for centuries. Various precautions have been taken to ensure this concept, which has a place as the right to privacy in many regulations. Articles in this context are included in the constitutions and criminal laws of the countries, and studies have been carried out to protect personal data through various regulations that the countries are subject to. Likewise, at the beginning of history, cryptology activities emerged among states to protect strategic information. Cryptological developments, which have experienced a snowball effect over the years, have become widespread and effective today.

Information Security Management Systems (ISMS) have been put into effect to protect corporate information security. It can be said that many precautions have been taken for corporate information security, thanks to the guides and standards regulating ISMS activities. Ensuring information security is of vital importance, especially for institutions operating in critical infrastructure sectors. Therefore, ISMS applications must be carried out carefully, especially in these institutions.

Although critical infrastructures vary from country to country, in line with the necessary examinations, it has been seen that the energy sector is considered the basic critical infrastructure sector for many countries. This situation is thought to be quite understandable since energy is a means of meeting human basic needs. In parallel, the high number of cyber-attacks against this sector also supports that. When we examine the attacks that have achieved their goals so far, it can be seen that their results are quite devastating. Therefore, ISMS applications should be adopted by

*Corresponding Author
Email addresses: maden.beyzanur@hotmail.com (B. Maden), alkan@gazi.edu.tr (M. Alkan)

everyone working in the sector and the defense mechanism against cyber-attacks should be strengthened by closing vulnerabilities whenever possible.

When the literature is examined, it is seen that no study has been conducted to measure any evaluation of ISMS from the perspective of people working in the energy sector in our country. This study was designed to fill the gap in the literature. In this context, it was thought that the survey study would be enlightening on the intriguing issue and various surveys were prepared.

In this study, first, a section with basic explanations about why ISMS is important for the energy sector is included. This section is followed by a section where some of the guides and standards for ISMS are mentioned. Then, the method of the study is included, and the details of the survey carried out are explained in the 'Method' section. The affiliated and relevant organizations of the Ministry of Energy and Natural Resources, which are the scope of the surveys, as well as the target audience of the surveys and the distribution of the number of participants, 181 in total, according to the surveys are also mentioned in this section. The survey results are shown in the 'Survey Analysis and Outputs' section. Finally, in the conclusion section, the analysis results and outputs are shared, and suggestions for improvement are presented.

2. The Importance of ISMS in the Energy Sector

Information security has now become a necessity for every institution and organization. This obligation comes to the fore, especially in critical infrastructure sectors. Since the energy sector is one of the critical infrastructures, a very sensitive process must be carried out in managing information security. ISMS is a system that ensures the protection of information within the framework of confidentiality, integrity, and accessibility, which are the three basic elements of information security, and manages processes that are based on continuity and open to continuous improvement. The system is based on the principle of running a cycle called "PDCA". The mentioned cycle is shown in Figure 1.

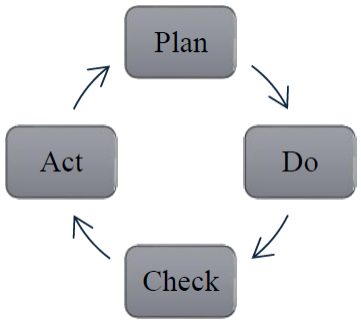

Figure 1. PDCA Cycle

At the "Plan" stage; the system is established by defining the scope, policies, procedures, and risks of the ISMS. The "Do" stage; is the phase of executing the system according to the decisions taken and the determined policies, procedures, and methods. The "Check" phase includes auditing the executed system and reporting its outputs. The "Act" phase is the phase that includes corrective and remedial activities. These stages should be implemented sequentially and repeated continuously.

In the most basic terms, it can be said that the aim is to protect corporate information security with the policies, procedures, and instructions established within the ISMS. The biggest share in achieving this goal falls on the staff of the institution. Human beings are the weakest link in the information security chain. It cannot be said that taking all necessary technical measures ensures complete protection of information security. With the high awareness of the institutional staff, corporate information security can be placed on a solid basis.

When the successful attacks that have occurred in the energy sector so far are examined, most of them occurred due to vulnerabilities caused by the human factor. Although the cyber security measures taken in technical terms are strong, seemingly simple mistakes such as falling into a phishing e-mail or inserting an unreliable external memory into the corporate computer weaken the entire system. As a result of vulnerabilities caused by simple errors, many situations occur, from the seizure of personal and corporate data to large-scale power outages. Some of the attacks on the energy sector that resulted in large-scale consequences and the years in which these attacks occurred are shown in Table 1.

Table 1. Some of the attacks on the energy sector

1982	Siberian natural gas pipeline explosion [10]
2003	Slammer worm infection at Davis -Besse nuclear power plant [11]
2009	Night Dragon attacks [17]
2010	Stuxnet attack on Natanz nuclear power plant [5]
2011	Attacks by the hacker group named Dragonfly [12]
2012	Shamoon virus attacks against Saudi Aramco and RasGas companies [6]
2012	Attack on Telvent company with a Trojan horse [20]
2014	Attack on Korean Hydro and Nuclear Power company [4]
2015	BlackEnergy attack on Ukrainian energy distribution companies [19]
2019	SCADA system attack at the power plant in the USA [1]
2020	Attack on wind turbines SCADA systems in Azerbaijan [1]
2023	Cosmicenergy malware to electric power disruption in Europe, Asia, and the Middle East [2]
2024	Ransomhub attacks on Matadero de Gijon bioenergy plant in Spain [3]

3. Information Security Guidelines and Standards

It is known that there are certain issues on which ISMS processes carried out to protect corporate information security are based. Activities organized in the light of some currently available guiding documents are provided with the certification of the same document. The most common information security certificate in our country is regulated by the International Organization of Standardization (ISO) and the International Electrotechnical Commission (IEC). ISO has been developing international standards on various issues since its establishment in 1947 and continues its activities with 171 member countries as of the date of preparation of this study [9]. On the other hand, IEC was founded in 1906 and prepares standards for areas under the umbrella of electrotechnology [7]. On behalf of our country, the Turkish Standards Institute (TSE), which has been operating since 1954, became a member of ISO in 1955 and of IEC in 1956 and took on the task of representation [18].

The information security standard in question is called ISO/IEC 27001. ISO/IEC 27001 is a certifiable standard belonging to the ISO/IEC 27000 family, which is described as the information security family. It was organized for the first time in 2005. In its current version in 2022, it includes information security, cyber security, and personal data security. ISO/IEC 27001 is a general standard with instructions applicable to all institutions and organizations. The instructions that must be followed are included in the "Annex A" section at the end of the standard. "Annex A" section edited in the 2022 version of the standard, has been turned into a document consisting of a total of 93 controls under four main headings and headings: institutional, personal, physical, and technological controls [8]. In the ISO/IEC 27002 standard, which is another standard of the ISO/IEC 27000 family, there are detailed explanations of the application principles of the ISO/IEC 27001 standard, namely "Annex A".

Within the scope of ISO/IEC 27001, audit activities are carried out for the institution once a year, depending on the certification processes. The validity period of the certificate is determined as 3 years. If no non-compliance is found that will lead to the cancellation of the certificate, audits; it is planned to include certification in the first year, a surveillance audit for the following 2 years, and a re-certification audit in the following year. There are standards within the ISO/IEC 27000 series that contain industry-specific information security instructions. One of these standards is the standard called "ISO/IEC 27019- Energy Service Industry Information Security Measures". ISO/IEC 27019 contains guidelines specific to the energy sector.

Established in 1901 as part of the United States Department of Commerce, the National Institute of Standards and Technology (NIST) is an institution that develops standards based on technology and measurement [14]. NIST has a series of standards for information security called NIST SP 800, similar to the ISO/IEC 27000 family. Belonging to the mentioned series; NIST SP 800-53 standard is named "Security and Privacy Controls for Information Systems and Organizations" and contains controls that contribute to the execution of information security processes with similar content to the ISO/IEC 27001 standard. However, in the NIST SP 800 series, there are customized standards as well as

standards that can be applied to all institutions and organizations, as in the ISO/IEC 27000 family. NIST SP 800-82 is one of these customized standards and is called "Guide for the Security of Operational Technologies".

The Information and Communication Security Guide was prepared and has been put into effect in our country in 2020 by the Presidential Digital Transformation Office of the Presidency of Türkiye. Within the guide, the processes that are carried out for the implementation of the guide, including planning, implementation, control, precaution-taking, and change management stages, are mentioned [15]. However, in the Guide, six asset groups were identified: "Network and System Security", "Application and Data Security", "Portable Device and Environment Security", "Security of Internet of Things (IoT) Devices", "Personnel Security", "Security of Physical Locations". The "Security Measures for Application and Technology Areas" and the "Tightening Measures" are also included.

Inspections are carried out for public institutions and organizations within the scope of the Guide. These audits must be carried out in accordance with the audit methodology determined in the Information and Communication Security Audit Guide published in 2021. The aforementioned methodology basically; includes the stages of planning the audit, implementing audit procedures, and reporting audit results [16]. Guide audits of Ministry of Energy and Natural Resources (MENR) affiliated and related organizations are carried out, if requested, by Ministry personnel who have the competence specified in the Guide regarding auditing.

4. Method

As stated in the Introduction section of the study, a survey was conducted to measure the perspective on ISMS activities in the sector. This study was finalized through the processes of determining the target groups of the surveys, preparing the questions, distributing the surveys, collecting the surveys, and evaluating the surveys. While determining the target groups for the preparation of the questions, the interest of the institutional staff in ISMS was considered. Like this, it was decided to prepare different questions for people responsible for carrying out ISMS activities in the institution, people who serve as managers in the institution, and people who do not have a role directly related to ISMS in the institution. In the continuation of the study, the survey groups are briefly listed as; "ISMS Employees", "Management" and "Personnel".

The survey questions were prepared for all three groups in general terms in line with the ISO/IEC 27001 standard. The reason for preparing different questions is that each personnel working within the institution has different responsibilities towards ISMS. For example, the standard includes a "Leadership" section where the duties of the top management towards ISMS are determined. While preparing the questions for the management survey, this section was taken as a priority along with other sections. The standard for the ISMS employee survey and personnel survey; sections such as "Policy", "Institutional roles, responsibilities, and authorities", "Competence", "Awareness", "Monitoring, measurement, analysis and evaluation" and "Improvement" were used. It was deemed appropriate to use a 5-point Likert scale for the survey. The answers to the questions in this regard are designed to be selected by ticking one of the options "Strongly Disagree", "Disagree", "Undecided", "Agree", or "Strongly Agree".

After the questions were prepared, the surveys were turned into an online form. Thus, the process of sending the links to the surveys to the relevant groups and presenting them to the participants was initiated. At this stage, it was necessary to determine a sample because it was not possible to study the entire Turkish energy sector, which was determined as the universe of the study. Distribution of all surveys was carried out with the permission and support of the Information Technology Department of the Ministry of Energy and Natural Resources (MENR). The link to the staff survey was sent to the MENR Information Technology Department staff via e-mail sent from the Presidency. In the same way, the ISMS Employees survey and the Management survey were sent to the MENR Central Organization and MENR affiliates and related organizations. The number of participants for the three surveys was determined to be 181 in total. 57 personnel participated in the Personnel survey, 77 personnel participated in the ISMS employee survey and 47 personnel participated in the Management survey. The analysis of the participants' responses is shown in the Findings section.

5. Survey Analysis and Outputs

After collecting the participants' responses, the necessary analyses were carried out through the SPSS program. Validity and reliability tests come first in these analyses. The compatibility of the variables within themselves is evaluated by Cronbach Alpha analysis. The reliability of the scale can be determined according to the value of Cronbach's Alpha coefficient (α) and;

- if $\alpha > 0$ and $\alpha \leq 0.40$, the scale is not reliable,
- if $\alpha > 0.40$ and $\alpha \leq 0.60$, the scale is less reliable,
- if $\alpha > 0.60$ and $\alpha \leq 0.80$, the scale is reliable,
- if $\alpha > 0.80$ and $\alpha \leq 1.00$, the scale is very reliable [13].

The results were obtained as $\alpha = 0.91321$ for the Personnel survey, $\alpha = 0.9658$ for the ISMS Employees survey, and $\alpha = 0.82185$ for the Management survey. Based on this, it can be said that the surveys are very reliable.

This section includes the analysis of Personnel, ISMS Employees, and Management surveys. For each question, there is the frequency (f) and percentage (%) of the option selected. Ratings were evaluated as; 1 point for the Strongly Disagree option, 2 points for the Disagree option, 3 points for the Undecided option, 4 points for the Agree option, and 5 points for the Strongly Agree option, and the average values were calculated based on these points. Firstly, Table 2 shows the analysis of the answers of the participants of the Personnel survey organized for employees within the MENR Information Technology Department who do not have a role directly related to ISMS activities.

Table 2: Analysis of personnel survey

	strongly disagree		do not agree		undecided		agree		strongly agree		Point	
	f	%	*f*	%	*f*	%	*f*	%	*f*	%	Average	Standard deviation
The information security management system is well implemented in the institution.	0	0.0	1	1.8	4	7.0	34	59.6	18	31.6	4.2	0.6
Awareness training is received within the scope of the information security management system standard.	0	0.0	1	1.8	7	12.3	32	56.1	17	29.8	4.1	0.1
The training provided on the information security management system is sufficient.	0	0.0	6	10.5	14	24.6	25	43.9	12	21.1	3.8	0.9
Thanks to the activities carried out within the scope of the information security management system, business processes are managed quickly and healthily.	0	0.0	1	1.8	13	22.8	30	52.6	13	22.8	4.0	0.7
Having an information security management system certificate for institutions and organizations doing business ensures information security.	2	3.5	5	8.8	10	17.5	26	45.6	14	24.6	3.8	1.0
The information security management system standard prevents violations of information security.	0	0.0	3	5.3	8	14.0	30	52.6	16	28.1	4.0	0.8
Activities carried out within the scope of the information security management system contribute to the realization of corporate risk analysis.	0	0.0	1	1.8	6	10.5	29	50.9	21	36.8	4.2	0.7

Continuation of Table 2

	strongly disagree		do not agree		undecided		agree		strongly agree		Point	
	f	%	*f*	%	*f*	%	*f*	%	*f*	%	Average	Standard deviation
Surveys are conducted to measure the quality of the information security management system.	0	0.0	9	15.8	11	19.3	25	43.9	12	21.1	3.7	1.0
Changes occurring within the scope of information security policy do not affect the current operation.	0	0.0	6	10.5	19	33.3	21	36.8	11	19.3	3.6	0.9
Information security management system policies are adopted and supported.	1	1.8	0	0.0	5	8.8	34	59.6	17	29.8	4.2	0.7
ISMS unit employees are in communication with personnel outside the team during the execution of information security management systems.	1	1.8	2	3.5	11	19.3	24	42.1	19	33.3	4.0	0.9

End of Table

Looking at the table, the number of participants who responded positively to the questions by marking the answers "agree" and "strongly agree" is higher. The average value, which can be at most 5, was calculated as 4 or above in 7 questions of 11 questions. It can be said that this situation is valid for all questions. Even in the question where the sum of the agree and strongly agree answers was the least compared to the other questions, the percentage of positive answers was calculated to be 56.1%. In this question, it was questioned whether the changes in ISMS policies had disrupted the order or not, and according to the analysis, a positive approach was concluded based on the general opinion that the order was not disrupted in most cases. It can be said that the analysis of the entire survey shows positive approaches to all of these survey questions. In general, it seems that the answers disagree and strongly disagree are quite few. On the other hand, it is noteworthy that the number of people who abstained from voting on some questions was high. In particular, the number of abstaining participants in the question mentioned in the paragraph above, which has the lowest percentage of positive answers, is 19. This question also has the distinction of being the question with the lowest average value, with 3.6.

Another survey that was analyzed is the ISMS Employees survey prepared for the personnel working in the ISMS unit of the MENR Central Organization, and the ISMS responsible of their own units, and the personnel working in the ISMS units of MENR affiliated and related organizations. The analysis table is given in Table 3.

Table 3: Analysis of the ISMS Employees survey

	strongly disagree		do not agree		undecided		agree		strongly agree		Point	
	f	%	*f*	%	*f*	%	*f*	%	*f*	%	Average	Standard deviation
Members of the information security management system unit are sufficient in number for the installation and execution of the system.	1.0	1.3	12	15.6	17	22.1	32	41.6	15	19.5	3.6	1.0
Institutional personnel are adequately equipped to establish and maintain the information security management system.	0	0.0	14	18.2	15	19.5	37	48.1	11	14.3	3.6	1.0
Consultancy services were received for the establishment of the information security management system.	1	1.3	6	7.8	24	31.2	31	40.3	15	19.5	3.7	0.9
ISMS Unit personnel have received training in order to carry out the processes properly in the information security management system.	1	1.3	6	7.8	12	15.6	35	45.5	23	29.9	3.9	0.9
The information security management system is carried out in cooperation with all institutional personnel.	3	3.9	6	7.8	14	18.2	38	49.4	16	20.8	3.8	1.0
Information security management system policies are prepared at a level that is understandable to everyone and communicated to all internal and external stakeholders, as well as to the institutional staff.	0	0.0	3	3.9	10	13.0	48	62.3	16	20.8	4.0	0.7
Information security management system policies are adopted by all employees within the institution.	0	0.0	14	18.2	21	27.3	32	41.6	10	13.0	3.5	0.9
Changes occurring within the scope of information security policy are not perceived by employees as a threat to the currently functioning system.	0	0.0	11	14.3	23	29.9	33	42.9	10	13.0	3.5	0.9
Having information security standards ensures corporate information security.	0	0.0	2	2.6	8	10.4	43	55.8	24	31.2	4.2	0.7

Continuation of Table 3

	strongly disagree		do not agree		undecided		agree		strongly agree		Point	
	f	%	*f*	%	*f*	%	*f*	%	*f*	%	Average	Standard deviation
Critical information security requirements within and outside the organization are met.	0	0.0	1	1.3	9	11.7	48	62.3	19	24.7	4.1	0.6
In the process after the information security certification, the institution's staff did not have difficulty adapting to the new rules.	0	0.0	11	14.3	24	31.2	34	44.2	8	10.4	3.5	0.9
The ISMS Unit is in communication with personnel outside the team during the execution of information security management systems.	0	0.0	6	7.8	11	14.3	48	62.3	12	15.6	3.9	0.8
All units are involved in a coordinated manner in the execution of the information security management system.	1	1.3	11	14.3	18	23.4	35	45.5	12	15.6	3.6	1.0
Within the scope of the information security management system, continuous improvements and updates are made.	0	0..	3	3.9	12	15.6	44	57.1	18	23.4	4.0	0.7
Necessary actions are taken in line with the outputs of the activities carried out to measure the quality of the information security management system.	0	0.0	1	1.3	13	16.9	49	63.6	14	18.2	4.0	0.6
Before the institution had the information security standard certificate, information security policies did not exist.	2	2.6	7	9.1	36	46.8	26	33.8	6	7.8	3.4	0.9
The information security standard certificate in the institution has caused a change in the information security policies before having the document.	0	0.0	2	2.6	23	29.9	40	51.9	12	15.6	3.8	0.7
After the information security management system was established, the security level increased compared to before.	1	1.3	0	0.0	8	10.4	47	61.0	21	27.3	4.1	0.7

Continuation of Table 3

	strongly disagree		do not agree		undecided		agree		strongly agree		Point	
	f	%	*f*	%	*f*	%	*f*	%	*f*	%	Average	Standard deviation
After the information security management system was established, there was a decrease in cyber-attacks against the institution compared to before.	1	1.3	4	5.2	30	39.0	27	35.1	15	19.5	3.7	0.9
After the information security management system was established, there was a decrease in personal and corporate data breaches compared to before.	0	0.0	0	0.0	17	22.1	42	54.5	18	23.4	4.0	0.7

End of Table

When Table 3 is examined, it seems that positive answers are dominant. The lowest average value was calculated to be 3.4. In the mentioned question, it was questioned whether information security policies existed before certification. In this question, there are more abstaining votes rather than fewer positive answers or more negative answers. It is thought that this situation may be due to a lack of information. In this regard, as a result of the investigations, it is noteworthy that the majority of abstention votes are generally high for all questions. Especially in the question about the intensity of cyber-attacks after ISMS, 30 people selected the "Undecided" option.

It is thought that there may be two reasons for this situation. The first of these is that the staff does not have enough information about the institution's history, and the second is that they are concerned that they may be disclosing information about the institution. The second possibility is thought to be less likely than the first. While preparing and distributing the surveys, care was taken not to process personal data or information about which institution they worked in, taking into account the free will of the participants, and this was informed to the participants.

When the first possibility is evaluated, considering that the processes related to the information security of the institution cover the past and the future, it is thought that it is essential to close the mentioned information gap immediately. This deficiency may be a result of excessive personnel turnover. In this case, the efforts that administrators must make to complete the deficiencies of the new staff regarding the institutional structure and background come to the fore.

The last survey analyzed is the Management survey. This survey was presented to the participation of employees in managerial positions in MENR Central Organization, MENR affiliated and related organizations. The analysis of the survey is shown in Table 4.

Table 4: Analysis of Management survey

	strongly disagree		do not agree		undecided		agree		strongly agree		Point	
	f	%	*f*	%	*f*	%	*f*	%	*f*	%	Average	Standard deviation
Having information security management system standards protects information security.	0	0.0	1	2.1	1	2.1	15	31.9	30	63.8	4.6	0.7
In case of a critical security problem, the information security management system provides protection.	0	0.0	3	6.4	1	2.1	17	36.2	26	55.3	4.4	0.8
Having internationally valid information security management system standards provides a national and international reputation.	0	0.0	0	0.0	3	6.4	15	31.9	29	61.7	4.6	0.6
Management plays an important role in implementing information security management system standards.	1	2.1	0	0.0	1	2.1	14	29.8	33	66.0	4.6	0.7
Information security management system policies are adopted by all employees within the institution.	0	0.0	5	10.6	10	21.3	18	38.3	14	29.8	3.9	1.0
All units are involved in information security management processes in a coordinated manner.	0	0.0	3	6.4	11	23.4	23	48.9	10	21.3	3.9	0.8
Within the scope of information security management, continuous improvements and updates are made.	0	0.0	0	0.0	3	6.4	25	53.2	19	40.4	4.3	0.6
Necessary actions are taken in line with the outputs of the activities carried out to measure the quality of the information security management system.	0	0.0	1	2.1	4	8.5	24	51.1	18	38.3	4.3	0.7
Top management controls and supports the information security management system.	0	0.0	1	2.1	2	4.3	21	44.7	23	48.9	4.4	0.7
The system operates properly in line with the approach of the senior management towards the information security management system.	0	0.0	0	0.0	3	6.4	22	46.8	22	46.8	4.4	0.6

Continuation of Table 4

	strongly disagree		do not agree		undecided		agree		strongly agree		Point	
	f	%	*f*	%	*f*	%	*f*	%	*f*	%	Average	Standard deviation
Senior management is not privileged from information security management system standard applications.	3	6.4	8	17.0	7	14.9	22	46.8	7	14.9	3.5	1.1

End of Table

When the answers to the management survey are examined, it is seen that the participants' perspective is extremely positive. 8 out of 11 questions have an average value of 4.3 or above. The lowest average value was calculated as 3.5. The number of negative answers to this question is higher than the other questions. At the same time, this question is also one of the questions that received the most abstaining votes. In the question, the privilege of the top management from ISMS applications was questioned. When the answers are evaluated, it can be stated that the question in question has a self-critical nature. The fact that some of the participants from the upper management, who are the target group of the survey, thought that they were privileged from various practices, provided an honest perspective on the system in evaluating the results. This situation may cause non-compliance in ISMS processes. Suggestions for precautions that can be taken in this context are also included in the conclusion section.

6. Conclusion

As one of the critical infrastructure sectors of the energy sector, violation of corporate information security is an issue that can be very dangerous for our country. Therefore, all kinds of research and studies on the processes carried out to protect information and the management of these processes based on a certain system are considered worthy of attention. It is thought that this study, which was conducted after detecting a deficiency in the literature on this issue, meets the expectations.

If necessary, investigations were made regarding the analysis of the surveys, it was seen that the perspectives of employees in the energy sector towards ISMS were shaped positively. ISMS, which is always open to improvement activities due to its structure, will continue its success if the right points are touched upon. In this regard, the most important studies that are considered appropriate for the energy sector are on awareness. Especially for personnel other than ISMS employees and those in managerial positions has been concluded that training aimed at contributing to the adoption of the purpose and basic requirements of ISMS will be very useful in raising awareness.

One of the issues that is considered important is that some of the senior management survey participants think that they are privileged from ISMS processes. Since these privileges are likely to create vulnerabilities, it is essential to manage privileges correctly. It is thought that it would be appropriate to minimize the privileges granted to senior management, put the granted privileges in writing along with policies and procedures, and follow them carefully.

Another issue that draws attention to the analysis is the issue of personnel shortage, which is a self-criticism made as a result of the ISMS employee survey analysis. If there are not enough personnel due to a high workload, the possibility of disruption of ISMS processes is considered dangerous. Therefore, based on the analysis of the surveys and the conclusion that the top management is open to taking responsibility for ISMS activities, it is thought that it will not be difficult to achieve improvements in this regard.

In conclusion, the system will be further strengthened by taking into account the necessary improvement activities on properly carried out ISMS processes in institutions in the energy sector.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this article.

Authors Contribution Statement

The authors have read and agreed the published version of the manuscript.

References

[1] Aydın, H., Barışkan, M.A., Çetinkaya, A., *Siber güvenlik kapsamında enerji sistemleri güvenliğinin değerlendirilmesi*, Güvenlik Bilimleri Dergisi, **10**(1)(2021), 151–174.

[2] Baran, G., COSMICENERGY – New OT Malware Causes Electric Power Disruption, Cyber Security News, 2023, Access address: https://cybersecuritynews.com/cosmicenergy-ot-malware/

[3] Baran, G., Ransomhub Attacking Industrial Control Systems To Encrypt And Exfiltrate Data. Cyber Security News, 2024, Access address: https://cybersecuritynews.com/cosmicenergy-ot-malware/

[4] Cohen, G., Throwback Attack: Korea Hydro Oath Nuclear Power Highlights the Vulnerability of Critical Systems, Industrial Cyber Security Pulse, 2023, Access address: https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-korea-hydro-and-nuclear-power-highlights-the-vulnerability-of-critical-systems/

[5] Dilipraj, E., *Supposed cyber attack on Kudankulam nuclear infrastructure — A benign reminder of a possibility reality*, Centre for Air Power Studies, **129**(2019), 1–5.

[6] Hemsley, K. E., Fisher, E., History of industry control system cyber incidents (No. INL/CON-18-44411-Rev002). Idaho National Lab. (INL), Idaho Falls, ID (United States), 2018.

[7] IEC. History. Access address: https://www.iec.ch/history, Access date:11/05/2024

[8] ISO/IEC 27001. (2022). Information Security Management Systems-Requirements.

[9] ISO. What we do. Access address: https://www.iso.org/what-we-do.html . Access date: 11/05/2024

[10] Kara, M., Cyber-Attacks-Cyber Wars and Their Effects, Master's Thesis, Institute of Social Sciences, İstanbul Bilgi University, 2013.

[11] Karabacak, B., Cyber threats to critical infrastructures and cyber security recommendations for Türkiye. Cyber Security Workshop, Information Security Association, Ankara, 29(2011), 1-11.

[12] Khan, F.B., Asad, A., Durad , H., Mohsin , S.M., Kazmi, S.N., *Dragonfly cyber-Threats: A case study of malware attacks targeting power grids*, Journal of Computing & Biomedical Informatics, **4(02)**(2023), 172–185.

[13] Kılıç, B., Information Security Management in Law Offices in Turkey in Terms of ISO/IEC 27001 Information Security Management System, Master's Thesis, Gazi University Informatics Institute, 2019.

[14] NIST. AboutNIST. Access address: https://www.nist.gov/about-nist . Access date:12/05/2024.

[15] Presidential Digital Transformation Office. (2020). Information and Communication Security Guide, 19-34. Ankara Türkiye.

[16] Presidential Digital Transformation Office. (2021). Information and Communication Security Audit Guide, 17th Ankara,Türkiye.

[17] Shull, A. (2014). Global cybercrime: the interplay of politics oath law. Organized Chaos: Reimagining the Internet, 97.

[18] TSE. Establishment of TSE. Access address: https://www.tse.org.tr/hakkimizda/. Access date:12/05/2024

[19] Yıldız, H., Anomaly Detection in Smart Grids Based on Software-Defined Networks Oath The Internet of Things, Master's Thesis, Sakarya University, 2023.

[20] Yenienerji. (2013). Telvent, Schneider More powerful with Electric. New energy. Access address: https://www.yenienerji.com/roportaj/telvent-schnneider-electric-ile-daha-guclu.