Volume 1 Nomor 1 | Juni 2023 | halaman 1-8

Inside | Jurnal Sistem Informatika Cerdas

Assessing Information Security Culture from an Individual's Viewpoint: A Quantitative Measurement Approach

Nur Andita Prasetyo[1*], Abdul Wahid[2], Fauzan Azim[3]
[123]Institut Teknologi dan Sains Mandala, Jember, Indonesia

Corresponding Author:
Nur Andita Prasetyo, Institut Teknologi dan Sains Mandala, Jember, 68121, Indonesia
Email: nurandita.prasetyo69@itsm.ac.id

Abstract

In the increasingly advanced digital era, information security has become a highly important aspect for organizations across various sectors. Therefore, organizations need to adopt a comprehensive approach to managing information security, which encompasses technological aspects, policies and procedures, as well as information security culture. Information security culture refers to the values, norms, and attitudes related to information security within an organization. This research aims to fill the knowledge gap by developing a quantitative measurement approach that can assess individuals' perspectives on information security culture in Sukowono District. This study is a quantitative research using the dimensions of awareness, knowledge, compliance, and behavior as questionnaire variables. The questionnaire was developed after determining the variables and tested for validity and reliability. The research was conducted in one of the districts in Jember Regency. The results of this study show that the average total score for Awareness is 11.9117647 with an average dimension score of 3.9705882, Knowledge has an average total score of 12 with an average dimension score of 4, Compliance has an average total score of 11.76470588 with an average dimension score of 3.92156863, and Behavior has an average total score of 11.882353 with an average dimension score of 3.960784. The dimensions are ranked from lowest to highest as follows: compliance, behavior, awareness, and knowledge. Therefore, knowledge of information security holds the highest position among the four dimensions, while the compliance dimension holds the lowest position.

Keywords : information security culture, information security awareness, behavior analysis, individual’s viewpoint, quantitative measurement approach

1 INTRODUCTION

In the increasingly advanced digital era, information security has become a critically important aspect for organizations across various sectors. Threats to information security, such as cyber attacks, data theft, and privacy breaches, are continuously increasing and can have detrimental impacts, including financial losses, damaged reputation, and loss of trust from customers and business partners [1]. Therefore, organizations need to adopt a comprehensive approach to managing information security, which encompasses technological aspects, policies and procedures, as well as information security culture [1,2].

Information security culture refers to the values, norms, and attitudes related to information security within an organization. A strong culture will influence individuals' behaviors related to information security, such as compliance with security policies, understanding of security threats, and active participation in security efforts [1]. Therefore, understanding information security culture from an individual's perspective is a critical factor in strengthening and enhancing information security within an organization [3].

Despite the importance of information security culture and individual roles in shaping it, there are still shortcomings in our understanding of individuals' perspectives on information security within organizations [2]. Some previous studies have focused on organizational information security culture aspects, but individual perspectives are often overlooked or inadequately examined. For example, many studies have primarily focused on the implementation of information security policies and the role of management, while individuals' perspectives related to information security have not received sufficient attention.

Measuring individuals' perspectives on information security culture is crucial for understanding the factors that influence individuals' attitudes and behaviors related to information security [3]. By understanding individual perspectives, organizations can develop more effective strategies to enhance compliance, awareness, and participation in information security initiatives. However, it is important to develop an appropriate measurement approach to assess individuals' views regarding information security culture [4].

In this context, this study aims to fill this knowledge gap by developing a quantitative measurement approach that can assess individuals' perspectives on information security culture in Sukowono District. Through the development of a valid and reliable measurement approach, this research is expected to make a significant contribution to understanding individuals' awareness, knowledge, compliance, and behavior related to information security within organizations. Additionally, this research will provide insights into the factors that influence information security culture from an individual perspective. Some individual factors related to information security culture include awareness, knowledge, compliance, and behavior.

The research method to be used in this study is a quantitative measurement approach. This approach will involve the development of a valid and reliable measurement instrument to collect data on individuals' perspectives regarding information security culture. The measurement instrument will include a set of questions designed to assess individuals' awareness, knowledge, compliance, and behavior related to information security.

The contribution of this research is expected to provide a better understanding of individuals' perspectives on information security culture. The findings of this research will offer valuable insights for organizations in designing more effective strategies to enhance individuals' awareness, knowledge, compliance, and behavior related to information security. Furthermore, this research can also provide a strong foundation for further studies in the field of information security culture.

2 RESEARCH METHOD

This methodology will enable researchers to collect valid and reliable data on individuals' perspectives regarding information security culture. By analyzing the data using appropriate statistical techniques, this study can provide valuable insights into the factors influencing awareness, knowledge, compliance, and behavior of individuals concerning information security [6]. The results of the data analysis can be used to identify common patterns and uncover the most influential factors in information security culture from an individual's perspective [5].

2.1. Definition of Research Variables

Identify the variables to be measured in this study, such as awareness, knowledge, compliance, and behavior of individuals related to information security. Develop clear operational definitions for each variable to ensure accurate measurement [3].

2.2. Development of Measurement Instruments

Design a questionnaire or measurement tool suitable for collecting data on individuals' perspectives regarding information security culture. This measurement tool should include relevant statements and provide the necessary data for analysis [4].

Table 1. Measurement Instrument

Dimension	Instruments
Awareness	[5]
	I am aware of my role and responsibility in information security.
	I am aware of the risks of not following information security policies.
	I am aware of the information security policies.
Knowledge	[6]
	I understand the importance of protecting personal, sensitive, and confidential information.
	I understand the negative consequences of information security issues.
	I am aware of the authority of Information Security within the organization.
Compliance	[6]
	Leaders communicate clear directions on protecting information to employees or third parties.

Behavior	I follow the established information security procedures/policies by the organization. I am aware of my role in information security but do not fully adhere to current practices. [6] I do not leave sensitive/secret information in insecure places. I regularly check documents for malware infections. I consider the negative consequences of their work before posting anything on social networking sites.

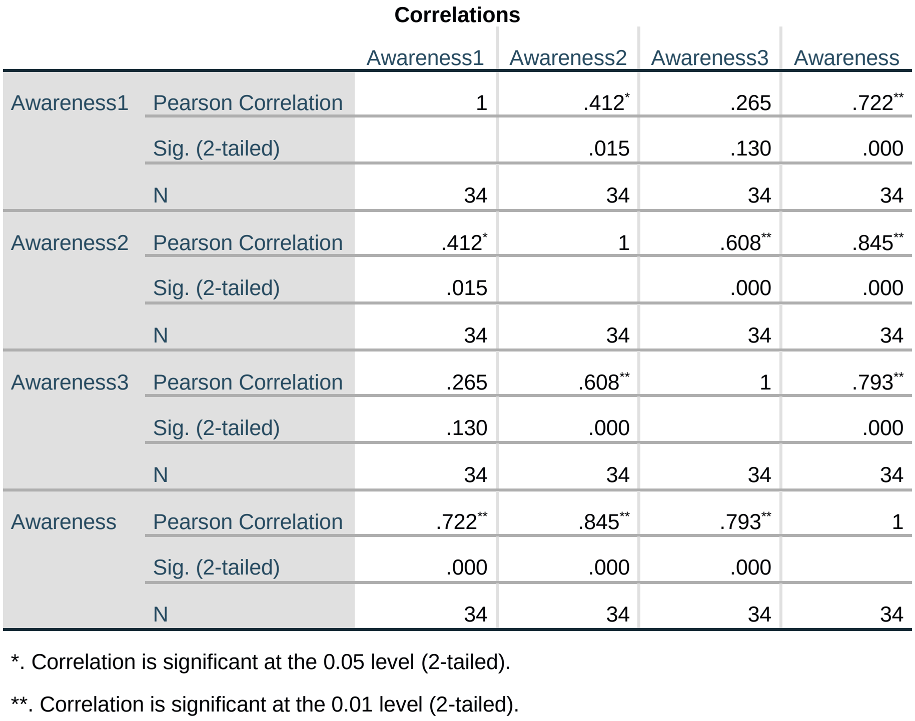
2.3. Validity and Reliability of Measurement Instruments

Conduct validity tests to ensure that the measurement instrument indeed measures the intended variables. Perform reliability tests to ensure that the measurement instrument is consistent in measuring the same variables [2].

2.3.1. Validity Test

The following are the results of the validity test for awareness, knowledge, compliance, and behavior based on 34 questionnaires filled out by employees of Sukowono District.

Table 2. Awareness Validity Test



Correlations

		Awareness1	Awareness2	Awareness3	Awareness
Awareness1	Pearson Correlation	1	.412*	.265	.722**
	Sig. (2-tailed)		.015	.130	.000
	N	34	34	34	34
Awareness2	Pearson Correlation	.412*	1	.608**	.845**
	Sig. (2-tailed)	.015		.000	.000
	N	34	34	34	34
Awareness3	Pearson Correlation	.265	.608**	1	.793**
	Sig. (2-tailed)	.130	.000		.000
	N	34	34	34	34
Awareness	Pearson Correlation	.722**	.845**	.793**	1
	Sig. (2-tailed)	.000	.000	.000	
	N	34	34	34	34

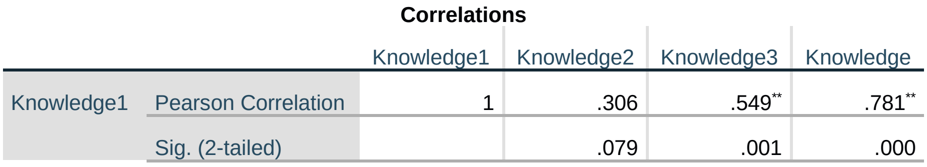
*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

*Decision Making Based on Sig. Value (2-tailed) with Significance of 0.05

Based on the "Correlations" output above, it is known that the Sig. value (2-tailed) for the relationship or correlation between Awareness1 and Awareness is 0.000 < 0.05, and the Pearson Correlation is positive with a value of 0.722 > 0.339. Therefore, it can be concluded that Awareness1 is valid. Similarly, the correlation between Awareness2 and Awareness is 0.000 < 0.05, and the Pearson Correlation is positive with a value of 0.845 > 0.339. Hence, it can be concluded that Awareness2 is valid. For the correlation between Awareness3 and Awareness, it is 0.000 < 0.05, and the Pearson Correlation is positive with a value of 0.793 > 0.339. Thus, it can be concluded that Awareness3 is valid. Since the items Awareness1, Awareness2, and Awareness3 are declared valid, these items can be used as accurate data collection tools in a research study.

Table 3. Knowledge Validity Test



Correlations

		Knowledge1	Knowledge2	Knowledge3	Knowledge
Knowledge1	Pearson Correlation	1	.306	.549**	.781**
	Sig. (2-tailed)		.079	.001	.000

.

	N	34	34	34	34
Knowledge2	Pearson Correlation	.306	1	.662**	.775**
	Sig. (2-tailed)	.079		.000	.000
	N	34	34	34	34
Knowledge3	Pearson Correlation	.549**	.662**	1	.898**
	Sig. (2-tailed)	.001	.000		.000
	N	34	34	34	34
Knowledge	Pearson Correlation	.781**	.775**	.898**	1
	Sig. (2-tailed)	.000	.000	.000	
	N	34	34	34	34

**. Correlation is significant at the 0.01 level (2-tailed).

*Decision Making Based on Sig. Value (2-tailed) with Significance of 0.05

Based on the "Correlations" output above, it is known that the Sig. value (2-tailed) for the relationship or correlation between Knowledge1 and Knowledge is 0.000 < 0.05, and the Pearson Correlation is positive with a value of 0.781 > 0.339. Therefore, it can be concluded that Knowledge1 is valid. Similarly, the correlation between Knowledge2 and Knowledge is 0.000 < 0.05, and the Pearson Correlation is positive with a value of 0.775 > 0.339. Hence, it can be concluded that Knowledge2 is valid. For the correlation between Knowledge3 and Knowledge, it is 0.000 < 0.05, and the Pearson Correlation is positive with a value of 0.898 > 0.339. Thus, it can be concluded that Knowledge3 is valid. Since the items Knowledge1, Knowledge2, and Knowledge3 are declared valid, these items can be used as accurate data collection tools in a research study.

Table 4. Compliance Validity Test

Correlations

		Compliance1	Compliance2	Compliance3	Compliance
Compliance1	Pearson Correlation	1	.579**	.275	.791**
	Sig. (2-tailed)		.000	.115	.000
	N	34	34	34	34
Compliance2	Pearson Correlation	.579**	1	.381*	.830**
	Sig. (2-tailed)	.000		.026	.000
	N	34	34	34	34
Compliance3	Pearson Correlation	.275	.381*	1	.718**
	Sig. (2-tailed)	.115	.026		.000
	N	34	34	34	34
Compliance	Pearson Correlation	.791**	.830**	.718**	1
	Sig. (2-tailed)	.000	.000	.000	
	N	34	34	34	34

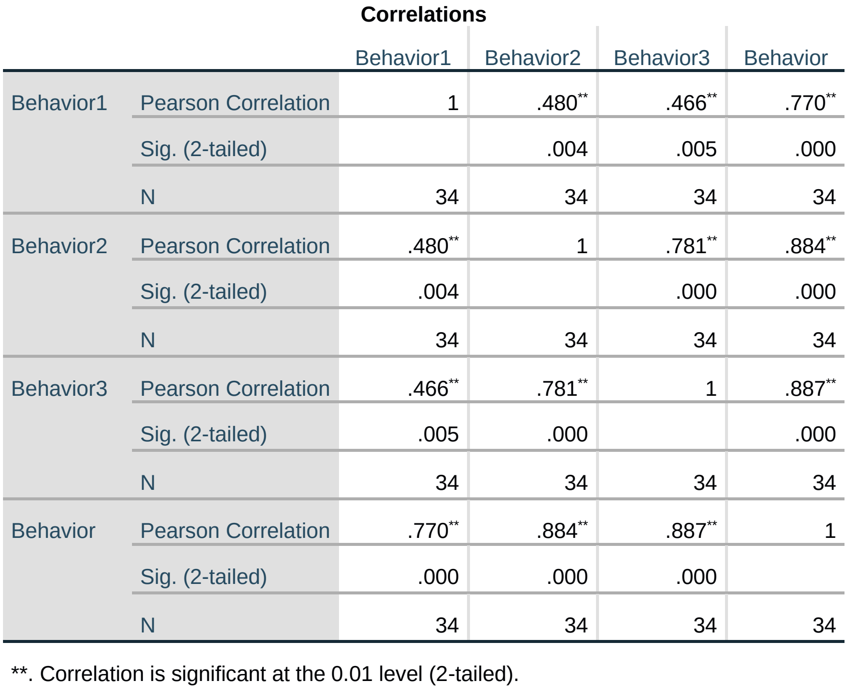
**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

*Decision Making Based on Sig. Value (2-tailed) with Significance of 0.05

Based on the "Correlations" output above, it is known that the Sig. value (2-tailed) for the relationship or correlation between Compliance1 and Compliance is 0.000 < 0.05, and the Pearson Correlation is positive with a value of 0.791 > 0.339. Therefore, it can be concluded that Compliance1 is valid. Similarly, the correlation between Compliance2 and Compliance is 0.000 < 0.05, and the Pearson Correlation is positive with a value of 0.830 > 0.339. Hence, it can be concluded that Compliance2 is valid. For the correlation between Compliance3 and Compliance, it is 0.000 < 0.05, and the Pearson Correlation is positive with a value of 0.718 > 0.339. Thus, it can be concluded that Compliance3 is valid. Since the items Compliance1, Compliance2, and Compliance3 are declared valid, these items can be used as accurate data collection tools in a research study.

Table 5. Compliance Validity Test



Correlations

		Behavior1	Behavior2	Behavior3	Behavior
Behavior1	Pearson Correlation	1	.480**	.466**	.770**
	Sig. (2-tailed)		.004	.005	.000
	N	34	34	34	34
Behavior2	Pearson Correlation	.480**	1	.781**	.884**
	Sig. (2-tailed)	.004		.000	.000
	N	34	34	34	34
Behavior3	Pearson Correlation	.466**	.781**	1	.887**
	Sig. (2-tailed)	.005	.000		.000
	N	34	34	34	34
Behavior	Pearson Correlation	.770**	.884**	.887**	1
	Sig. (2-tailed)	.000	.000	.000	
	N	34	34	34	34

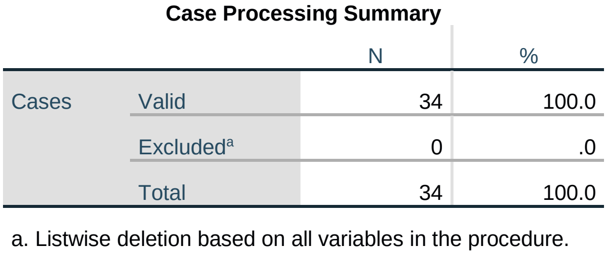
**. Correlation is significant at the 0.01 level (2-tailed).

*Decision Making Based on Sig. Value (2-tailed) with Significance of 0.05

Based on the "Correlations" output above, it is known that the Sig. value (2-tailed) for the relationship or correlation between Behavior1 and Behavior is 0.000 < 0.05, and the Pearson Correlation is positive with a value of 0.770 > 0.339. Therefore, it can be concluded that Behavior1 is valid. Similarly, the correlation between Behavior2 and Behavior is 0.000 < 0.05, and the Pearson Correlation is positive with a value of 0.884 > 0.339. Hence, it can be concluded that Behavior2 is valid. For the correlation between Behavior3 and Behavior, it is 0.000 < 0.05, and the Pearson Correlation is positive with a value of 0.887 > 0.339. Thus, it can be concluded that Behavior3 is valid. Since the items Behavior1, Behavior2, and Behavior3 are declared valid, these items can be used as accurate data collection tools in a research study.

2.3.2 Reliability Test

Table 6. Case Processing Summary



Case Processing Summary

		N	%
Cases	Valid	34	100.0
	Excluded[a]	0	.0
	Total	34	100.0

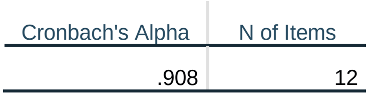
a. Listwise deletion based on all variables in the procedure.

The table above provides information about the sample size or respondents (N) analyzed in the SPSS program, which is N = 34 individuals. Since there is no missing data (meaning all respondent answers are filled), the valid count is 100%.

Table 7. Reliability Test

Reliability Statistics

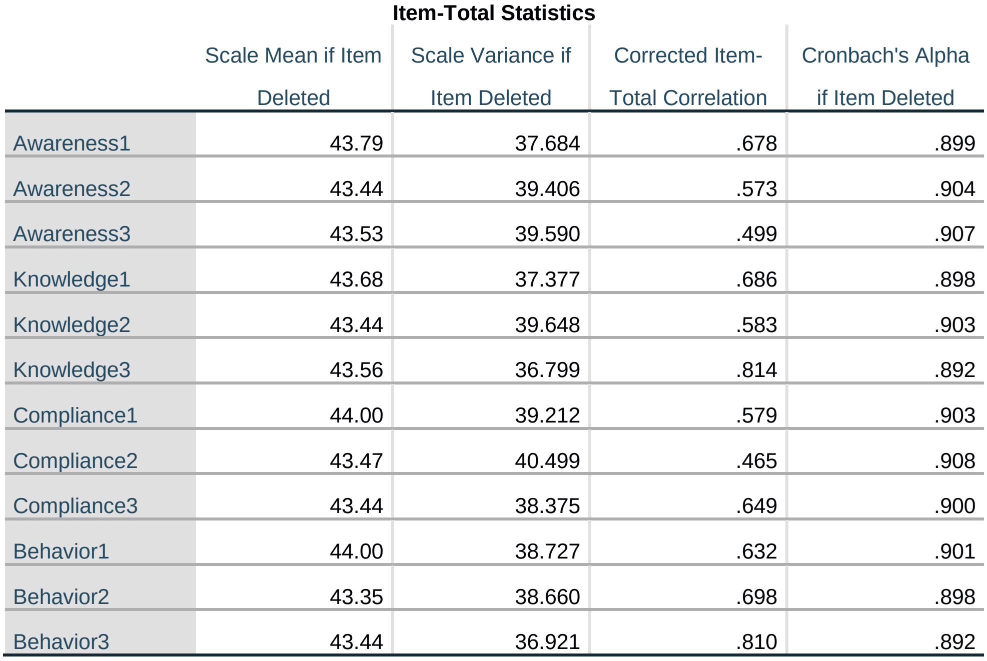
.



Cronbach's Alpha	N of Items
.908	12

From the table above, it is known that there are N of Items (number of questionnaire items) which is 12 items, with a Cronbach's Alpha value of 0.908. Since the Cronbach's Alpha value is 0.908 > 0.60, it can be concluded that all 12 items of the questionnaire statements are reliable or consistent.

Table 7. Correlation Test



Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Awareness1	43.79	37.684	.678	.899
Awareness2	43.44	39.406	.573	.904
Awareness3	43.53	39.590	.499	.907
Knowledge1	43.68	37.377	.686	.898
Knowledge2	43.44	39.648	.583	.903
Knowledge3	43.56	36.799	.814	.892
Compliance1	44.00	39.212	.579	.903
Compliance2	43.47	40.499	.465	.908
Compliance3	43.44	38.375	.649	.900
Behavior1	44.00	38.727	.632	.901
Behavior2	43.35	38.660	.698	.898
Behavior3	43.44	36.921	.810	.892

In the column "corrected item-total correlation," items with values below 0.3 are items that can be considered for elimination. This procedure can be found in the book "Penyusunan Skala Psikologi" by Pak Azwar (2012). In the column "Cronbach's Alpha if item deleted," this value indicates the Cronbach's Alpha value if that item is deleted. Items with higher Cronbach's Alpha values when deleted can be considered for elimination. This procedure can be found in the book "Nunally" (1978).

2.4. Data Collection

Determine the population that will be the subjects of the research. In this study, the researcher selects one district as the respondents. Collect data by distributing questionnaires to randomly selected respondents. Ensure that respondents understand the instructions and questions in the questionnaire [8].

2.5. Data Analysis

Use appropriate statistical analysis techniques to analyze the data obtained from the questionnaires. Descriptive analysis will be used to summarize characteristics and common patterns in the data. Factor analysis or principal component analysis can be used to identify dimensions or underlying factors of the measured variables [7].

2.6. Interpretation of Results

Interpret the results of data analysis by considering significant findings and emerging patterns [10].

3 RESULTS AND ANALYSIS (11 PT)

3.1. Results and Analysis

Table 7. Results

Dimension	Mean Total Scores	Mean Dimension Scores
Awareness	11,9117647	3,9705882
Knowledge	12	4
Compliance	11,76470588	3,92156863

Behavior	11,882353	3,960784

The table above presents the mean total scores and mean dimension scores for each dimension from the perspective of individuals towards the organizational security culture, namely, awareness, knowledge, compliance, and behavior. The dimension of awareness has a total mean score of 11.9117647 and a dimension mean score of 3.9705882. The dimension of knowledge has a total mean score of 12 and a dimension mean score of 4. The dimension of compliance has a total mean score of 11.76470588 and a dimension mean score of 3.92156863. Lastly, the dimension of behavior has a total mean score of 11.882353 and a dimension mean score of 3.960784.

3.2. Discussion

The results of this study indicate that individuals have a positive attitude towards information security within the organization. They are aware of the importance of information security and demonstrate a high level of knowledge regarding information security. Individual perspectives on information security are influenced by factors such as awareness, knowledge, compliance, and behavior [1]. The higher these factors are, the stronger the information security culture that is formed.

Several studies have revealed that information security training has a significant impact on individuals' perceptions of information security culture [7, 8, 9]. Effective training can enhance individuals' awareness, knowledge, compliance, and behavior related to information security [8, 10]. Additionally, organizational support plays an important role in shaping the information security culture [11]. Organizations that provide strong support in terms of resources, clear policies, and commitment to information security tend to have a better information security culture [7, 9].

The findings of this research have important implications for information security practices within organizations. It is crucial for organizations to develop comprehensive and effective information security training programs to enhance individuals' knowledge and awareness [10]. Organizations should also provide strong support in terms of policies and adequate resources to establish a solid information security culture [11]. This can be achieved by implementing clear policies, providing sufficient resources to implement those policies, and ensuring high commitment from management and all members of the organization towards information security [12].

Information security culture is not something static but needs to be continuously maintained and updated [13]. This study suggests that ongoing training and effective communication about information security are important to maintain individuals' awareness and compliance with security policies. Organizations need to continue their efforts in strengthening the information security culture by adopting sustainable approaches, such as conducting regular training, raising awareness campaigns, and involving all members of the organization in safeguarding information security [14].

4 CONCLUSION

In this research, the dimensions in Sukowono District are ranked from the lowest to the highest as follows: compliance, behavior, awareness, and knowledge. Therefore, knowledge of information security holds the highest position among the three other dimensions, while the compliance dimension holds the lowest position among the three other dimensions. In this regard, decisive actions related to policies are needed to enhance the value of the compliance dimension.

REFERENCES

[1] B. S. Nur Andita Prasetyo, "Kajian Dimensi Budaya Keamanan Informasi dalam Berbagai Organisasi," Jurnal Teknologi Rekayasa, vol. 7, pp. 73-82, 2022.

[2] A. da Veiga and N. Martins, "Improving the information security culture through monitoring and implementation actions illustrated through a case study," Computers & Security, pp. 162-176, 2015.

[3] Nasir, R. A. Arshah and M. R. A. Hamid, "Information Security Policy Compliance Behavior Based on Comprehensive Dimensions of Information Security Culture: A Conceptual Framework," Information System and Data Mining, pp. 56-60, 2017.

.

[4] Al Hogail, "Design and validation of information security culture framework," Computers in Human Behavior, pp. 567-575, 2015.

[5] M. A. Alnatheer, "Understanding and Measuring Information Security Culture in Developing Countries: Case of Saudi Arabia," PhD diss., Queensland University of Technology, 2012.

[6] P. K. Sari, A. Prasetio, Candiwan, P. W. Handayani, A. N. Hidayanto, S. Syauqina, E. F. Astuti and F. P. Tallei, "Information security cultural differences among health care facilities in Indonesia," Heliyon, vol. 7, no. 6, 2021.

[7] Nasir, R. A. Arshah and M. R. A. Hamid, "A dimension-based information security culture model and its relationship with employees' security behavior: A case study in Malaysian higher educational institutions," Information Security Journal: A Global Perspective, vol. 28, no. 3, pp. 55-80, 2019.

[8] T. O. Nævestad, S. F. Meyer and J. H. Honerud, "Organizational information security culture in critical infrastructure: Developing and testing a scale and its relationships to other measures of information security," in Safety and Reliability, London, Taylor & Francis Group, pp. 3021-3029, 2018.

[9] A. Nasir, R. A. Arshah, M. R. A. Hamid and S. Fahmy, "An analysis on the dimensions of information security culture concept: A review," Journal of Information Security and Applications, pp. 12-22, 2019.

[10] S. Orehek and G. Petrič, "A systematic review of scales for measuring information security culture," Information and Computer Security, pp. 133-158, 2021.

[11] M. A. Alnatheer, "Understanding and Measuring Information Security Culture in Developing Countries: Case of Saudi Arabia," PhD diss., Queensland University of Technology, 2012.

[12] P. K. Sari, A. Prasetio, Candiwan, P. W. Handayani, A. N. Hidayanto, S. Syauqina, E. F. Astuti and F. P. Tallei, "Information security cultural differences among health care facilities in Indonesia," Heliyon, vol. 7, no. 6, 2021.

[13] T. R. Vinnakota and N. G. P. L Mandaleeka, "Assessing an Information Security Governance of an Enterprise," US Patent, 2017.

[14] M. N. Masrek, Q. N. Harun and M. K. Zaini, "The Development of an Information Security Culture Scale for the Malaysian Public Organization," International Journal of Mechanical Engineering and Technology (IJMET), p. 1255–1267, 2018.

[15] Choe, A. I. Al-Darwish and Pilsung, "A Framework of Information Security Integrated with Human Factors," International Conference on Human- Computer Interaction, p. 217–229, 2019.

[16] K. Arbanas and N. Z. Hrustek, "Key Success Factors of Information Systems Security," Journal of Information and Organizational Sciences, pp. 131-144, 2019. [37] Z. Shouran, T. K. Priyambodo and A. Ashari, "Information System Security: Human Aspects," International Journal of Scientific & Technology Research, pp. 111-115, 2019.