Appropriate Sets of Criteria for Innovation Adoption of IS Security in Organizations

Sandy Kosasi
STMIK Pontianak
Pontianak, West Kalimantan, Indonesia
sandykosasi@yahoo.co.id

Vedyanto
Santu Petrus Junior High School
Pontianak, West Kalimantan, Indonesia
vedy91@gmail.com

I Dewa Ayu Eka Yuliani
STMIK Pontianak
Pontianak, West Kalimantan, Indonesia
dewaayu.ekayuliani@gmail.com

***Abstract*—Determining sets of criteria and alternatives becoming main priorities is essential to guarantee the success of innovation adoption of Information System (IS) security. The goal of this research was to select and determine important entities as representation of each criterion for managers in making decisions of innovation adoption of IS security. This research applied Technology-Organization-Environment (TOE) Framework, and Human-Organization-Technology-Fit (HOT-Fit) Model to map relative importance variables of criteria and alternatives. AHP Approach was applied for computation simulation to determine priorities of criteria and alternatives. Results show that a principal criterion is manpower of organizations. The eigen factor score is 4.398. Moreover, alternatives covering complexity, financial resources, intensity of competition, and CIO innovativeness have these respective eigen factors scores: 4.326, 9.307, 4.376, and 4.545.**

Keywords—IS Security; Innovation Adoption; TOE Framework; HOT-Fit Model; AHP Approach

I. INTRODUCTION

IS (Information System) security becomes an old problem of any organizations. It is an inherent part of all organizational activities. Even small weaknesses of IS can bring failure of organizational operation [1]. Therefore, more organizations cooperate to get ISO certificate of IS security like ISO27001 [2]. Securing IS is the challenge of each organization since data security as well as availability and integrity of information are immensely influenced by complexity of environmental changes, interrelationships, uncertainties, and dependencies on Information Technology (IT). Securing IS can be actualized through determination of policies, procedures, and mechanisms of information flows of organizational structures to prevent exploitation of vulnerability of threats and risks [3].

Moreover, applying IS security system is influenced by capabilities to adopt innovation of IS security for organizational needs. The reason is that each organization has dissimilar characteristics of work culture which is in line with certain needs of IS security [4]. Most organizations only rely on renewal of security and individual willingness to make new trials without analyzing the needs appropriately [5]. Innovation adoption of IS security is a complex process. Consequently, numerous organizations face difficulties of applying steps with policies, procedures, and mechanisms properly. Besides, steps of developing and implementing IS security adopted by individuals and organizations are still low [6]. Thus, it is of great importance to comprehend why users accept or reject organizational IS security [7].

There have been previous studies discussing innovation adoption of IS security. However, literature specifically exploring models of innovation adoption of IS security in certain organizational levels is rare to find. Previous studies mostly emphasize needs of building and maintaining competitive, operational strengths of IS security. Effectiveness of innovation adoption of IS security is prone to depend on humans, technology, and policies through TOE Framework [8]. Innovation adoption of IS security is strategic and brings significant effects on the success of implementing IS through relationships of humans, technology, organizations, and environment [9]. However, the lack of preparation of understanding adoption of IS security can become primary hindrance of achieving the success of securing the IS assets [10]. In addition, TOE Framework is frequently used and maximized in adopting innovation of IS security in organizations. IS security is also an internal need and involves external parties when representing the systematic innovation adoption of IS security [11].

Adoption innovation of IS security in organizations fails if there are mistakes of determining sets of criteria appropriately [12]. Applying this adoption requires careful considerations of selecting sets of criteria with critical, strategic roles based on specification of organizational needs [13]. It is noted that complexity of selecting and determining sets of criteria exists as organizations have different management and behavior [13]. This statement is supported by previous studies affirming that most organizations only seek easiness by making

978-1-5386-8402-3/18/$31.00 ©2018 IEEE

replication of existing models directly without strategic considerations of organizational contents [14, 15, 16, 17].

Such the occurrence creates the failure since it is admitted that all criteria are the same and can contribute to conformity of innovation adoption of IS Security. Therefore, in order to make this process successful, strategic decision making is needed to determine proper and important sets of criteria and alternatives for organizations. Different organizations can have different strategic decisions.

Needs of criteria in this research applied dimensions of TOE Framework [18, 19]. They were completed with HOT-Fit Model [20] consisting of technology, organizations, environment, and humans. Meanwhile, alternatives (relative advantage, compatibility, complexity, security concern, presence of champions, infrastructure, top management support, organizational size, financial resources, mimetic pressure, coercive pressure, intensity of competition, vendor support, perceived technical competence of IS staff, employees' IS knowledge, clinical IT experts, and CIO innovativeness) used the variable of each dimension [21, 22].

The research aimed to select and determine sets of criteria which are the most appropriate with the most important alternatives as representation of categories of criteria based on TOE Framework and HOT-Fit Model. This was to ensure readiness of applying innovation adoption of IS security. In order to determine decisions on mainly prioritized factors, AHP Approach method was used.

AHP Approach is also an alternative way to solve various kinds of problems of organizational needs. It can be used to represent decision makers' views of individual institutions. AHP Approach focuses on changes due to different hierarchies created by different people. This method gives 3 advantages such as implementation of empirical cases leading to intuitive solutions, complexly manipulated results, and relative importance of numerous criteria [23].

Computation through AHP Approach is hierarchical when representing functional types of interrelationships. Therefore, complicated cases with multi-criteria can be decomposed into detailed decision elements. Hierarchical models are linearly structured from common decision elements until the most concrete, controllable factors at each bottom level in the form of a decision alternative [24]. Benefits of AHP Approach are that: (a) hierarchical structures as consequences of selected criteria and subcriteria are deep; (b) validity can be computed with the limitation to inconsistent tolerance of selected criteria and alternatives; (c) output tenacity through analyses of sensitivity is measureable [25].

II. Theoretical Background

Information is a principal asset of organizations and requires protection. It is crucial for organizations to secure all IS assets due to possible malicious attacks and unauthorized use of access [26]. Protection of the whole IS assets is the form of anxiety because it brings significant impacts on sustainability of organizational activities, and develops and implements system [27]. Protective actions include the use of antivirus, firewall, filter, intrusion detection system, encryption, authorization mechanisms, authentication system, and proxy devices. Furthermore, providing the training and education on IS security system can help to eliminate IS threats [28].

Possessing IS security is compulsion. Each organization must always secure information assets. IS security should have orientation on perspectives for users. It expedites transaction and exploration of decision making. The foci are security, availability, and integrity [29]. As the consequence, system vulnerability is enhanced [30]. Nonetheless, assuring the success of adoption and implementing IS security in organizations can be actualized through combination of complex practices of TOE Framework and HOT-Fit Model. In fact, full commitment of the whole staff and management levels of organization units is needed [31]. Previous scientific contributions sustainably indicate that the weakest tab of each plan or IS security procedure is the use of computers per se [32].

Implementation of each model of innovation adoption of IS security pertains to strategic decisions of mapping and determining essential sets of criteria based on characteristics and attitude of organizations [33]. Adoption of IS security is fundamental. It should be actualized in organizations. Based on perception of models of innovation adoption of IS security, organizational and individual levels should be analyzed [34].

III. Research Method

The source of data was the survey through the use of questionnaires sent to all selected respondents by using online, electronic media. This research involved analysis units of organizations. The eighty-five respondents were managers or directors of IT department of palm oil plantation industries working in West Kalimantan Province. Purposive sampling technique was in use to collect data. The computation was through Likert Scales [35]. Data obtained from online questionnaires were completed with in-depth interviews [35]. In order to enhance validity and reliability of collected answers, these interviews were conducted with several selected respondents in groups. The communication was through the application of Whatsapp.

Results of processed data were analyzed by using AHP Approach. This is to support steps of strategic decision making and appropriate sets of criteria of IS security adoption. This approach creates the form of simulation enabling the best choice of sets of criteria and alternatives. Such the model is in forms of hierarchical structures of criteria and alternatives, and is considered through inconsistent tolerance and analysis of sensitivity [36]. The first step is calculation covers definition of problems, goals, and final results. Other steps comprise decomposition of problems in forms of hierarchies and decision elements, paired comparison of decision elements in forms of matrices, estimation of relative weight of decision elements, and examination of hierarchical consistency [37].

The goals need to be divided into subgoals with specific measurement. The hierarchies include goals, criteria or objective levels, and alternatives. Every set of criteria can further be divided into more detailed levels. After all criteria are identified, scores are related to above levels. Relative

scores obtained for choices are measured based on hierarchical levels. Next, scores are synthesized through models. Composite scores of choices at levels and overall scores appear as a result of this process. The measurement is relative for each level and produces matrix scores. However, the results should be consistent. Thus, examination of inconsistency should be conducted to find out and identify possibilities of mistakes of data inputs. A matrix (i,j) is considered to be consistent if the whole elements follow transitivity. Guidelines showing whether Consistency Index (CI) have consistent matrices should exist (see Table I) [38].

TABLE I. BASIC SCALES OF THE ORDER OF IMPORTANCE

Order of Importance	Definition
1	As important as others
3	Moderately important
5	Strongly important
7	Very strongly important
9	Extremely important
2,4,6,8	Scores between two adjacent computations
Reciprocal	If Element i has one of the scores above in comparison to Element j, Element j has a reverse score.

A matrix created as a result of random comparison is absolutely inconsistent. The limit of stated inconsistency is measured through Consistency Ratio (CR). Comparison of CI and Random Index (RI) produces reference scores and determines consistency levels of matrices. CR is computed with this formula: CR = CI/RI (see Table II). Meanwhile, CI is obtained through this formula: CI = $(\lambda max-n)/n-1$. However, RI is the stated average of consistency becoming the standard of computation of CR. Next, CR of paired matrices is examined. If CR is greater than 0.1, paired comparison should be recalculated until CR is less than or equals to 0.1 [39, 40].

TABLE II. AVERAGES OF CONSISTENCY (RI)

N	RI
1	0.00
2	0.00
3	0.58
4	0.90
5	1.12
6	1.24
7	1.32
8	1.41
9	1.45
10	1.49
11	1.51
12	1.48
13	1.56
14	1.57
15	1.59

IV. RESULTS AND DISCUSSION

Determination of sets of criteria and alternatives started with formulation and determination of a number of criteria through previous results using TOE Framework and HOT-Fit Model. All criteria referred to research results [21, 22]. They were processed again to produce the order of importance. Main criteria were initially considered.

The order of importance of criteria was related to palm oil plantation industries in West Kalimantan Province. The adoption success of IS security referred to combination of TOE Framework and HOT-Fit Model with dimensions of Technology (T), Organization (O), Environment (E), and Human (H). Meanwhile, the variables were (1) relative advantage, (2) compatibility, (3) complexity, (4) security concern, (5) presence of champions, (6) infrastructure, (7) top management support, (8) organizational size, (9) financial resources, (10) mimetic pressure, (11) coercive pressure, (12) intensity of competition, (13) vendor support, (14) perceived technical competence of IS staff, (15) employees' IS knowledge, (16) clinical IT experts, and (17) CIO innovativeness. These seventeen instruments were alternatives of criterion (see Figure 1).

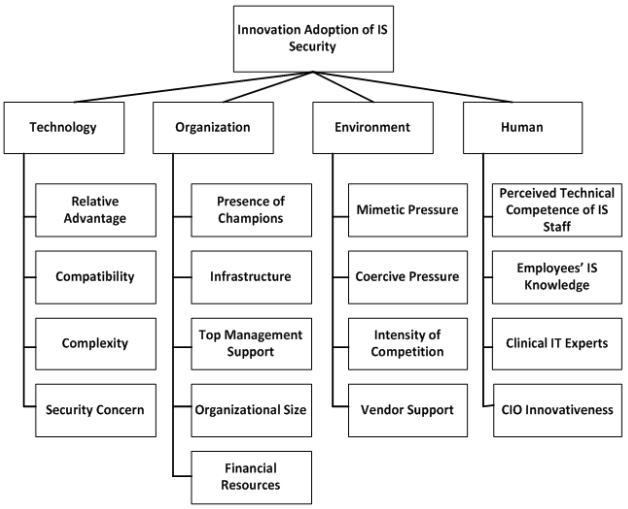

Fig. 1. Hierarchy Model of Criteria and Alternatives

The model of multicriteria combining TOE Framework and HOT-Fit Model began with paired comparison applied to determine weight of criteria and alternatives measured based on subjective preferences of decision making. Comparative Scales 1-9 were used. Next, examination of consistency of paired comparison matrices was conducted. If the ratio is greater than 0.1, paired comparison should be recalculated until it is less than or equals to 0.1 (consistent). Similar steps were applied to comparison matrices among alternatives. Following these, totals of multiplication results of weight of criteria and alternatives were sought.

Outcomes of hierarchical criteria of (a) technology and organization, (b) technology and environment, (c) technology and human, (d) organization and environment, (e) organization and human, and (f) environment and human are consecutively 0.053, 0.057, 0.136, 0.086, 0.182, and 0.136. After conducting

the calculation, eigen factors of technology (0.084), organization (0.175), environment (0.224), and human (0.517) appear. CR levels of all criteria were measured afterwards to indicate comparison of valid results and actual conditions. CR is comparison of CI and RI. CI is obtained through this formula: CI = (λmax-n)/n-1, whereas RI is the score determined with AHP Approach. 4x4 matrices used in this research should have scores which are less than 9%. RI used is 0.90.

Based on computation, it is found that CI equals to 0.071 (7.08%) and CR equals to 0.079 (7.87%). Therefore, strategic decisions of IS security adoption should firstly emphasize human or manpower in comparison to other criteria. As it can be seen from Table III, obtained eigen factors of human criterion is 4.398. Referring to calculation results, the human criterion possesses the highest score. Thus, innovation adoption of IS security requires mapping of organizational staff's abilities to be in line with factors of technology, organization, and environment.

TABLE III. MEASUREMENT OF CRITERION CONSISTENCY

Criterion	T	O	E	H	Total	Summary
T	0.084	0.058	0.075	0.129	0.346	4.111
O	0.253	0.175	0.112	0.172	0.712	4.078
E	0.253	0.349	0.224	0.129	0.955	4.263
H	0.337	0.524	0.896	0.517	2.274	4.398
Total	0.927	1.105	1.307	0.948	4.287	16.849
L-Max						4.212

Every criterion has a different probability level based on business patterns of societies. People's readiness and willingness to accept changes of system and mechanisms of adoption of IS security are priorities. The willingness should be strengthened with strong motivation to accept and implement IS security for the success of organizations. Also, it is important for the staff to have technical skills of IT so that conformity of perception of business needs and IS security exists. The staff should further have mastery of knowledge on structures and mechanisms when securing IS assets. Moreover, there should be security experts improving staff's knowledge. Hence, the staff can work with updated IT in clear organizational structures and controlled environment. Next, consistency of the whole alternatives referring to criteria was measured.

Based on calculation of the eigen factor of technology criterion, obtained scores of these variables: Relative Advantage (R), Compatibility (C1), Complexity (C2), and Security Concern (SC) are respectively 0.070, 0.170, 0.288, and 0.472. Meanwhile, CI = 0.063 and CR = 0.070 (6.95%) result in acceptance. A strategic decision of technology criterion is on complexity with eigen factor = 4.326. Other strategic decisions of security concern, compatibility, and relative advantage can be seen from Table IV.

TABLE IV. COMPARISON OF ALTERNATIVES BASED ON TECHNOLOGY CRITERION

Technology Alternatives	R	C1	C2	SC	Total	Summary
R	0.070	0.043	0.096	0.079	0.287	4.100
C1	0.280	0.170	0.096	0.157	0.704	4.132
C2	0.210	0.511	0.288	0.236	1.245	4.326
SC	0.420	0.511	0.575	0.472	1.979	4.192
Total	0.981	1.235	1.055	0.944	4.214	16.751
L-Max						4.188

Next, in terms of organization criterion, eigen factors of Presence of Champions (PC) (0.395), Infrastructure (I) (0.239), Top Management Support (TMS) (0.163), Organizational Size (OS) (0.120), and Financial Resources (FR) (0.084) were found. Other outcomes show that CI = 0.010 and CR = 0.009 (0.91%) resulting in acceptance. A strategic decision on organization criterion is on financial resources with eigen factor = 9.307. Other strategic decisions of presence of champions, infrastructure, organizational size, and top management support are indicated in Table V.

TABLE V. COMPARISON OF ALTERNATIVES BASED ON ORGANIZATION CRITERION

Organization Criterion	PC	I	TMS	OS	FR	Total	Summary
PC	0.395	0.717	0.978	0.040	0.042	2.171	5.502
I	0.132	0.239	0.652	0.060	0.021	1.103	4.617
TMS	0.066	0.060	0.163	0.024	0.042	0.354	2.175
OS	0.132	0.119	0.033	0.120	0.028	0.431	3.604
FR	0.197	0.060	0.081	0.359	0.084	0.781	9.307
Total	0.921	1.195	1.906	0.602	0.217	4.841	25.204
L-Max							5.041

Following these, measurement of alternative consistency of environment criterion shows that eigen factors of Mimetic Pressure (MP), Coercive Pressure (CP), Intensity of Competition (IC), and Vendor Support (VS) are consecutively 0.099, 0.171, 0.277, and 0.453. CI = 0.010 and CR = 0.009 (0.91%) indicate acceptance. A strategic decision of environment criterion is on intensity of competition with eigen factor = 4.376. It is continued with vendor support, coercive pressure, and mimetic pressure (see Table VI).

TABLE VI. COMPARISON OF ALTERNATIVES BASED ON ENVIRONMENT CRITERION

Environment Criterion	MP	CP	IC	VS	Total	Summary
MP	0.099	0.057	0.139	0.113	0.408	4.121
CP	0.297	0.171	0.092	0.151	0.711	4.163
IC	0.198	0.512	0.277	0.226	1.214	4.376
VS	0.396	0.512	0.555	0.453	1.916	4.232
Total	0.990	1.253	1.064	0.943	4.249	16.892
L-Max						4.223

Finally, measurement of alternative consistency of human criterion yields eigen factors of Perceived Technical Competence of IS Staff (PTCISS), Employees' IS Knowledge (EISK), Clinical IT Experts (CITE), and CIO Innovativeness (CIOI) are 0.091, 0.153, 0.217, and 0.538 in order. Meanwhile, CI = 0.075 and CR = 0.083 (8.28%) were found and acceptance was confirmed. A strategic decision of human criterion is on CIO innovativeness with eigen factor = 4.545. Others are clinical IT experts, perceived technical competence of IS staff, and employees' IS knowledge (see Table VII).

TABLE VII. COMPARISON OF ALTERNATIVES BASED ON HUMAN CRITERION

Human Criterion	PTCISS	EISK	CITE	CIOI	Total	Summary
PTCISS	0.091	0.077	0.072	0.135	0.375	4.100
EISK	0.183	0.153	0.108	0.179	0.624	4.067
CITE	0.274	0.307	0.217	0.108	0.906	4.182
CIOI	0.366	0.460	1.083	0.538	2.448	4.545
Total	0.915	0.998	1.480	0.960	4.352	16.894
L-Max						4.224

V. CONCLUSION AND FUTURE RESEARCH

Research results were used to explore and determine sets of criteria and alternatives becoming priorities of innovation adoption of IS security. Through AHP Approach, the most crucial criteria are readiness and capabilities of the human to conduct such adoption and most crucial criteria with eigen factor 4.398 area readiness. However, the most essential alternatives are complexity, financial resources, intensity of competition, and CIO innovativeness with these respective eigen factors 4.326, 9.307, 4.376, and 4.545.

All of these variables are principal criteria and, therefore, should be seriously concerned to adopt innovation of IS security especially for palm oil plantation industries in West Kalimantan Province. Orders of criteria and alternatives should be applied as they are name of changes are allowed. Sets of criteria are inappropriate for other industries. This research can be enhanced through engagement of more specific respondents based on clusters of management levels in organizations.

REFERENCES

[1] D. Tunçalp, "Diffusion and Adoption of Information Security Management Standards across Countries and Industries," Journal of Global Information Technology Management, Taylor & Francis Group, 17, 2014, pp. 221-227.

[2] International Organization for Standardization (ISO), "The ISO survey of certifications," Retrieved from https://isotc.iso.org/livelink/livelink/fetch/-8853493/8853511/8853520/18808772/00.Executive_summary_2016_Survey.pdf?nodeid=19208898&vernum=-2

[3] A.E.D. Albuquerque Junior, and E.M.D. Santos, "Adoption of Information Security Measures in Public Research Institutes," JISTEM-Journal of Information Systems and Technology Management, 12(2), 2015, pp. 289-315.

[4] S. Chatterjee, S. Sarker, and J.S. Valacich, "The Behavioral Roots of Information Systems Security: Exploring Key Factors Related to Unethical IT Use," Journal of Management Information Systems, 31(4), 2015, pp. 49-87.

[5] K. Hwang, and M. Choi, "Effects of Innovation-Supportive Culture and Organizational Citizenship Behavior on E-Government Information System Security Stemming from Mimetic Isomorphism," Government Information Quarterly, 34(2), 2017, pp. 183-198.

[6] M.A. Hameed, and N.A.G. Arachchilage, "A Conceptual Model for the Organisational Adoption of Information System Security Innovations," Journal of Computer Engineering & Information Technology, 6(2), 2017, pp. 1-10.

[7] J. Shropshire, M. Warkentin, and S. Sharma, "Personality, Attitudes, and Intentions: Predicting Initial Adoption of Information Security Behavior," Computers & Security, 49, 2015, pp. 177-191.

[8] T. Herath, H.S. Herath, and J. D'Arcy, "Managing Security in Organizations: Adoption of Information Security Solutions," SIGMIS-CPR, 2017, pp. 87-88.

[9] H. Ahmadi, O. Ibrahim, and M. Nilashi, "Investigating a New Framework for Hospital Information System Adoption: A Case on Malaysia," Journal of Soft Computing and Decision Support Systems, 2(2), 2015, pp. 26-33.

[10] M.A. Hameed, and S. Counsell, "Assessing the Influence of Environmental and CEO Characteristics for Adoption of Information Technology in Organizations," Journal of Technology Management and Innovation 7(1), 2012, pp. 64-84.

[11] M.A. Hameed, and N.A.G. Arachchilage, "A Model for the Adoption Process of Information System Security Innovations in Organisations: A Theoretical Perspective," Australasian Conference on Information Systems, 2016, pp. 1-12.

[12] K.P. Kiilu, D.M. Nzuki, "Factors Affecting Adoption of Information Security Management Systems: A Theoretical Review," International Journal of Science and Research (IJSR), 5(12), 2016, pp. 162-166.

[13] H. Ahmadi, M. Nilashi, O. Ibrahim, T. Ramayah, M.W. Wong, M., Alizadeh, ... and A Almaee, "Exploring Potential Factors in Total Hospital Information System Adoption," Journal of Soft Computing and Decision Support Systems, 2(1), 2015, pp. 52-59.

[14] O.J. Opala, and S.M. Rahman, "An Exploratory Analysis of the Influence of Information Security on the Adoption of Cloud Computing," 8th International Conference on Systems Engineering (SoSE), IEEE, 2013, pp. 165-170.

[15] R. Baskerville, P. , Spagnoletti, and J. Kim, "Incident-Centered Information Security: Managing a Strategic Balance between Prevention and Response," Information & Management, 51(1), 2014, pp. 138-151.

[16] M. Nilashi, H. Ahmadi, A. Ahani, O. Ibrahim, and A. Almaee, "Evaluating the Factors Affecting Adoption of Hospital Information System Using Analytic Hierarchy Process," Journal of Soft Computing and Decision Support Systems, 3(1), 2016, pp. 8-35.

[17] H. Gangwar, H. Date, and A.D. Raoot, "Review on IT Adoption: Insights from Recent Technologies," Journal of Enterprise Information Management, 27(4), 2014, pp. 488-502.

[18] L.G. Tornatzky, and M. Fleischer, "The Processes of Technological Innovation," Lexington Books Lexington, MA, 1990.

[19] J. Baker, "The Technology–Organization–Environment Framework," Information Systems Theory, Springer, 2012.

[20] M.M. Yusof, J. Kuljis, A. Papazafeiropoulou, L.K. Stergioulas, "An Evaluation Framework for Health Information Systems: Human, Organization and Technology-Fit Factors (HOT-Fit)," Int. J. Med. Inform, 77(6), 2008, pp. 386–398.

[21] M. Nilashi, H. Ahmadi, A. Ahani, R. Ravangard, and O. bin Ibrahim, "Determining the Importance of Hospital Information System Adoption Factors Using Fuzzy Analytic Network Process (ANP)," Technological Forecasting and Social Change, 111, 2016, pp. 244-264.

[22] H. Ahmadi, M. Nilashi, and O. Ibrahim, "Organizational Decision to Adopt Hospital Information System: An Empirical Investigation in the Case of Malaysian Public Hospitals," International Journal of Medical Informatics, 84(3), 2015, pp. 166-188.

[23] R. Sharda, D. Delen, and E. Turban, "Business Intelligence and Analytics: Systems for Decision Support," Tenth Edition, Prentice-Hall, Inc., 2014.

[24] P. Kishore, and G. Padmanabhan, "An Integrated Approach of Fuzzy AHP and Fuzzy TOPSIS to Select Logistics Service Provider," Journal for Manufacturing Science and Production, 16(1), 2016, pp.51-59.

[25] V.L. Sauter, "Decision Support Systems for Business Intelligence," Second Edition, John Wiley & Sons, Inc., 2011.

[26] N.A.G. Arachchilage, C. Namiluko, and A. Martin, "A Taxonomy for Securely Sharing Information among Others in a Trust Domain," 8th International Conference for Internet Technology and Secured Transactions (ICITST), IEEE, 2013, pp. 296-304.

[27] Q.J. Yeh, and A.J.T. Chang, "Threats and Countermeasures for Information System Security: A Cross-Industry Study," Information & Management, 44(5), 2012, pp. 480-491.

[28] N.A.G. Arachchilage, S. Love, and K. Beznosov, "Phishing Threat Avoidance Behaviour: An Empirical Investigation," Computers in Human Behavior, 60, 2016, pp. 185-197.

[29] Z.A. Soomro, M.H. Shah, and J. Ahmed, "Information Security Management Needs More Holistic Approach: A Literature Review," International Journal of Information Management, 36(2), 2016, pp. 215-225.

[30] A. Vance, P.B. Lowry, and D.W. Wilson, "Using Trust and Anonymity to Expand The Use of Anonymizing Systems that Improve Security across Organizations," Security Journal, 30(3), 2017, pp. 979-999.

[31] H. Ahmadi, M. Nilashi, L. Shahmoradi, and O. Ibrahim, "Hospital Information System Adoption: Expert Perspectives on an Adoption Framework for Malaysian Public Hospitals," Computers in Human Behavior, 67, 2017, pp. 161-189.

[32] P. Gillingham, "Decision-Making about the Adoption of Information Technology in Social Welfare Agencies: Some Key Considerations," European Journal of Social Work, 2017, pp. 1-9.

[33] Z. Yang, A. Kankanhalli, B.Y. Ng, and J.T.Y. Lim, "Analyzing the Enabling Factors for the Organizational Decision to Adopt Healthcare Information Systems," Decision Support Systems, 55(3), 2013, pp. 764-776.

[34] E. Ziemba, "The ICT Adoption in Enterprises in the Context of the Sustainable Information Society," Federated Conference on Computer Science and Information Systems (FedCSIS), IEEE, 2017, pp. 1031-1038.

[35] J.W. Creswell, "Research Design: Qualitative, Quantitative, and Mixed Methods Approaches," Fourth Edition, California: SAGE Publications, Inc., 2014.

[36] T.L. Saaty, "Decision Making For Leaders: The Analytic Hierarchy Process for Decisions in a Complex World," Third Revised Edition, RWS Publications, 2012.

[37] M.S. Pieter, I.I. Lamia, and F.Y. Wattimena, "Decision Support System in Giving Recommendation for Flat Screen Television Purchase Using Analytical Hierarchy Process Method," Second International Conference on Informatics and Computing (ICIC), IEEE, 2017, pp. 1-5.

[38] S. Lee, W. Kim, Y.M. Kim, and K.J. Oh, "Using AHP to Determine Intangible Priority Factors for Technology Transfer Adoption," Expert Systems with Applications, 39(7), 2012, pp. 6388-6395.

[39] C.N. Castillo, F.K. Degamo, F.T. Gitgano, L.A. Loo, S.M. Pacaanas, N. Toroy, ... and C.O. Ocampo, "Appropriate Criteria Set for Personnel Promotion Across Organizational Levels Using Analytic Hierarchy Process (AHP)," International Journal of Production Management and Engineering, 5(1), 2017, pp. 11-22.

[40] U. Yudatama, B.A. Nazief, and A.N. Hidayanto, "Strategic Decisions in the Implementation of Information Technology Governance to Achieve Business and Information Technology Alignment Using Analytical Hierarchy Process," Information Technology Journal, 16(2), 2017, pp.51-61.