JNEST EISSN: 2961-8738 ● PISSN: 2961-8916 ● DOI: 10.56741/jnest.v1i01.57
Article Received 30 June 2022. Revised 25 July 2022.

Assessment and Mitigation of Information Security Policy in Budgeting System using KAMI Index 4.1

Tawar*, Imam Riadi, Adiniah Gustika Pratiwi, Ariqah Adliana Siregar

***Abstract*—This Threats to information resources require information security management policies in every agency. The Information Security Index (KAMI Index) is one of the methods developed by the Ministry of Communication and Information Technology, used to evaluate the maturity level, completeness of ISO/IEC 27001:2013 implementation and information security readyness. As a national zakat institution, XYZ Organization has utilized information technology in several systems, including the budgeting system. However, the information security index has never been measured. This condition may result in the risk of threats to information security, so it is necessary to measure. The Budgeting System needs to be measured using KAMI Index 4.1. The assessment criteria are carried out on seven categories to know how the quality of the information security policy is. The results of this assessment, XYZ organization gets an electronic system score is 17, governance 75, risk management 30, framework 31, asset management 37, ICT 38, securing third party involvement 40%, service security 20%, personal data protection 27% so the total score of 5 categories is 211 or at level I+ to II. This organization has started implement the framework at early stage and has not met the initial requirements for ISO/IEC 27001:2013 certification.**

***Index Terms*—assessment, information, KAMI index, security, charity institution**

I. INTRODUCTION

THE development of information technology (IT) every day is advancing very rapidly. Due to this development, the entire organization or company must adapt and implement IT advancements[1]. Charity Organization XYZ is one of the organizations that implement IT advances. This organization is a national-level zakat institution trusted to manage zakat funds, infaq, waqf, and other philanthropic funds, both individuals, institutions, companies, and other agencies. This agency is intended as a zakat management institution with modern management that can deliver zakat to be part of the social problem solver that continues to grow.

There are six pillars of the program run by Charity Organization XYZ, namely education, health, economy, social humanity, da'wah, and the environment. This Charity agency also has several selected donation programs, including zakat, infaq, programs, and qurban, but they don't accept any form of funds originating from crime.

Charity Organization XYZ has several systems in managing zakat funds, one of which is a budgeting system with the system has risks and gaps in information security. The system needs to analyze and evaluate the level of readiness (completeness and maturity) of its security implementation. The existence of a threat to these information resources requires the presence of an information security management in every agency, including government-owned public service providers[2]. Information security describes efforts to protect computers and non-computers, data facilities, and information from misuse by irresponsible people[3].

In the implementation of ICT governance, the information security factor is a crucial aspect to consider considering that the performance of ICT governance will be disrupted if information as one of the main objects of ICT governance experiences problems in the form of interference and threats concerning aspects of confidentiality, integrity, and availability (availability). The Ministry of Communication and Information Technology of the Republic of Indonesia has issued regulation number 4 of 2016 concerning Information Security Management Systems (ISMS)[4]. As a form of implementation of the applicable law, the Ministry of Communication and Information (Kemkominfo) of the Republic of Indonesia expects organizations that operate electronic systems to carry out SNI ISO 27001 certification related to information security[5]. Several assessment tools can be used regarding information security in institutions, for example, by using ISO 27001:2013[6], COBIT[7], a combination of COBIT 4.1, ITIL v.3, and ISO 27001[8].

The National Standardization Agency was established on April 8, 2016, SNI ISO/IEC 27001:2013 as the national standard in information technology. To obtain a standardized measure of SNI ISO/IEC 27001:2003, the National Cyber and Crypto Agency (BSSN) issued an application that is used as a tool to analyze and evaluate the level of readiness (completeness and maturity) of the application of SNI ISO/IEC 27001:2003, namely the KAMI Index (Information Security Index)[9].

The Information Security Index (KAMI) is one of the methods developed by the Ministry of Communication and Informatics, used to evaluate the maturity level, the completeness of the implementation of ISO/IEC 27001:2013, and the readiness of information security[10]. The KAMI index is not intended to analyze the feasibility or effectiveness of existing forms of protection, but rather as a tool to provide an overview of the state of readiness of the information security framework to the leadership of corporate agencies[11] Thus, Charity Organization XYZ needs to apply the KAMI Index (Information Security) as a tool to analyze and evaluate the level of security readiness by the criteria in SNI ISO/IEC 27007.

The authors are with the Information Systems Department of Ahmad Dahlan University Yogyakarta, Indonesia (Corresponding Author's email: tawar@is.uad.ac.id).

II. Literature Review

A. *Information Security*

Information security is an effort to prevent fraud (cheating)[12] or detect fraud in information-based systems, where the information itself has no physical meaning Information security that exists today can become a necessity for an organization because security in knowledge is a fundamental problem in a business[13].

Information security is intended to maintain the Confidentiality aspect, Integrity, and Availability of information when accessed. Figure 1 describes the elements of information security[14].

Fig. 1. Information security aspects.

Correlation between threats and vulnerabilities, namely weaknesses that exist in the system that these threats can exploit. Efforts to reduce the vulnerability aspects in the system can also reduce threats to the system[15] . Several information security methods are used to minimize and manage risks to information security. These methods include Risk Assessment, Maturity Level to assess the level of information security that has been implemented by the organization and implement information security policies to regulate and manage information security.

B. *Information Security Management Standard*

Information Security Management Standard (ISMS) is a goal in achieving the goals of an organization by establishing, implementing, using, monitoring, reviewing, maintaining, and improving information security[16].

Standard ISO (International Organization for Standardization) has developed many standards on Information Security Management System (ISMS) since 2005 in requirements and guidelines. From the ISO 27000 series standard, up to September 2011, only ISO/IEC 27001:2005 has been adopted National Standardization Agency (BSN) as Indonesian National Standard (SNI) Indonesian language numbered SNI ISO/IEC 27001:2009 [17].

C. *ISO 27001*

ISO 27001 is a standard intended to assist companies in protecting the security of company assets and protecting the Information Security Management System (ISMS). ISO 27001 is a standard issued by International Organization for Standardization[18]. ISO 27001 provides a framework for the scope of information technology and asset management in ensuring that the information security established within an organization is by SNI [19]. ISO 27001 has the advantage that the ISO 27001 standard is very flexible depending on the organization's needs[20]. The ISO 27001 standard is independent of information technology products, requires the use of a risk-based management approach, and is designed to ensure that the selected security controls can protect information assets from various risks and provide confidence in the level of security for interested parties[21]. The organizational structure in ISO 27001 is divide into two:

1) Clausul (*Mandatory prosess).* The organization must meet requirements if implementing the ISMS (Information Security Management System).
2) Annex A (*security control).* The reference document can be used to determine the security controls that need to be established in the ISMS (Information Security Management System)[22].

D. *KAMI Index*

KAMI Index is an evaluation tool to analyze an organization's information security level of readiness. This evaluation tool is not intended to explore the feasibility or effectiveness of existing forms of security but rather to provide an informative description of the state of readiness (completeness and maturity) of an organization's framework[23].

The form of evaluation applied by the Index is made so that it can be used by organizations of various levels, sizes, and levels of importance in using ICT in supporting the implementation of existing processes.

KAMI Index evaluation process can be used by organizations on a national scale and small. The evaluation process is carried out through many questions in each of the areas below:

1) Category of Electronic System used by Agencies
2) Information security governance category
3) Information Security Risk Management
4) Information Security Framework
5) Asset management category
6) Information Technology and Security
7) Suplement: Evaluation area for aspects of Third Party Engagement Security, Cloud Service Security and personal data protection.

The initial stage before the quantitative assessment process is carried out is to carry out a classification process for the Electronic Systems used with the aim of grouping the Electronic Systems used into certain "levels": Low, High, Strategic.

TABLE I
ELECTRONIC SYSTEM CATEGORY MATRIX

Electronic System Category				
Low		**Final Score**		**Readiness Status**
		0	174	Not Feasible
10	15	175	312	Fulfillment of the basic framework
		313	535	Pretty good
		536	645	Good
High		**Final Score**		**Readiness Status**
		0	272	Not Feasible
16	34	273	455	Fulfillment of the basic framework
		456	583	Pretty good
		584	645	Good
Strategic		**Final Score**		**Readiness Status**
		0	333	Not Feasible
35	50	334	535	Fulfillment of the basic framework
		536	609	Pretty good
		610	645	Good

Based on Table I, the Electronic System category matrix shows the final score, which will be adjusted to the readiness status of the Agency or Organization for information security. The evaluation process in each area of KAMI Index discusses aspects in achieving the primary goal of securing the site. The form of security using minimum readiness is required for the SNI ISO/IEC 27001:2013 standard certification process. The following is a score mapping table for self-assessment and forms a matrix between security category statuses[24].

TABLE II
KAMI INDEX SECURITY CATEGORY

Security Category			
Security Status	**1**	**2**	**3**
Not done	0	0	0
In planning	1	2	3
In progress	2	4	6
Fully applied	3	6	9

In Table II, the evaluation process respondents are asked to provide responses starting from areas related to the form:

1) Label 1 : Information Security Basic Framework
2) Label 2 : Effectiveness and Consistency of Its Application
3) Label 3 : Ability to Improve Information Security Performance [25].

The next grouping is based on the maturity level of the security application, which refers to the maturity level used by the COBIT or CMMI framework. The maturity level will be used to report the mapping and ranking of information security readiness in the Organization.

Based on Fig. 2, the maturity level is defined as:

1) Level I - Initial Condition
2) Level II - Implementation of the Basic Framework
3) Level III - Defined and Consistent
4) Level IV - Managed and Scalable
5) Level V - Optimal

The above maturity levels are added with levels between I+, II+, III+, and IV+, so there are nine levels of maturity in total. Based on the ISO/IEC 27001:2013 standard, the expected maturity level as the minimum certification threshold is Level III+.

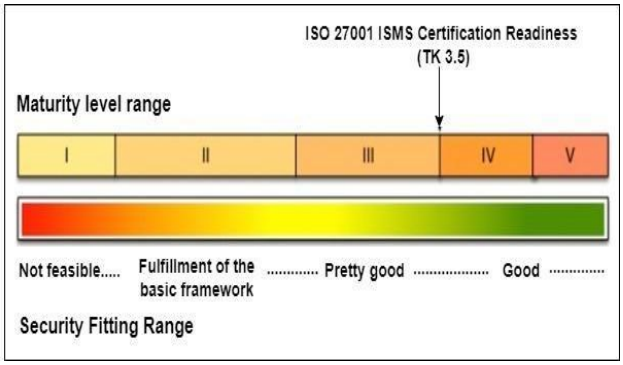

Fig. 2. Completeness and maturity level.

III. METHOD

This research assesses the level of information security in an organization using KAMI Index 4.1 method. Fig. 3 depicts the research flow and the following explanation

There were several steps. FGD (Focus Group Discussion) with Organization XYZ is the initial process in the literature study. The FGD was conducted to find out the problems regarding the existing system and what method would be used in this research. After getting the results from the FGD, the next step is to determine or choose what method can solve the problems. The literature study was carried out by reviewing previous research which was relevant to the research to be carried out and then selecting the KAMI Index 4.1 method according to the ISO/IEC 27001 standard to solve the problems found.

The next stage is to collect data by filling out the KAMI Index questionnaire conducted by selected respondents (responsible IT staff & and other related staff) according to the questionnaire category. Questionnaire KAMI Index, which is used in the latest version of 4.1.

The next stage is data validation by confirming to the respondents to ensure the data provided is in its original state. Confirmation of this data is done by online meeting using Zoom Meeting application with respondents and asks for evidence in related documents (if any) in each area. Data analysis is a step for calculating the questionnaire results and analyzing the level of readiness (completeness and maturity) of information security in the budgeting system. The next stage is presenting the results by conducting an FGD with Organization XYZ The last stage is concluding the results of the research conducted. These results are then compared with the control in ISO 27001. After that, the following process is the recommendation process to provide input on deficiencies that the agency has not carried out.

IV. RESULTS AND DISCUSSION

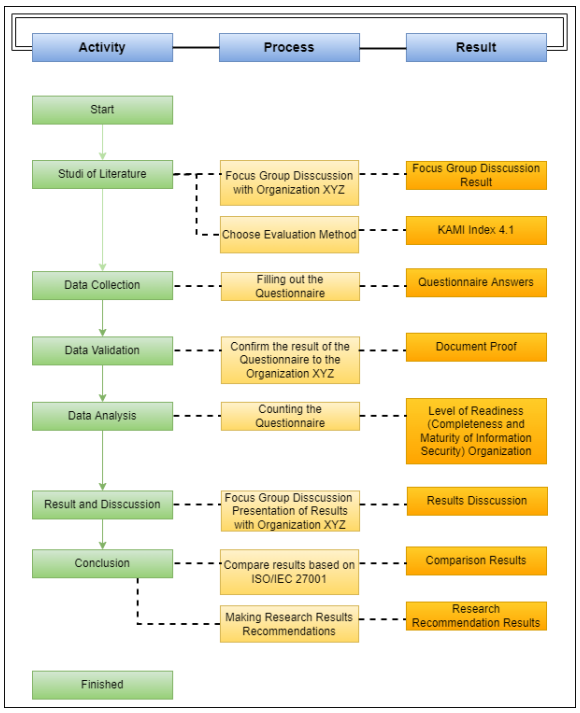

Fig. 3. Research methodology.

The results of the evaluation of the level of readiness (completeness and maturity) of information security in the budgeting system are grouped into seven category areas according to KAMI Index version 4.1. These categories include Electronic Systems, Information Security Governance, Information Security Risk Management, Information Security Management Framework, Information Asset Management, Information Technology, and Security and Supplements. The evaluation results from the seven categories are shown in the dashboard KAMI Index in Fig. 4.

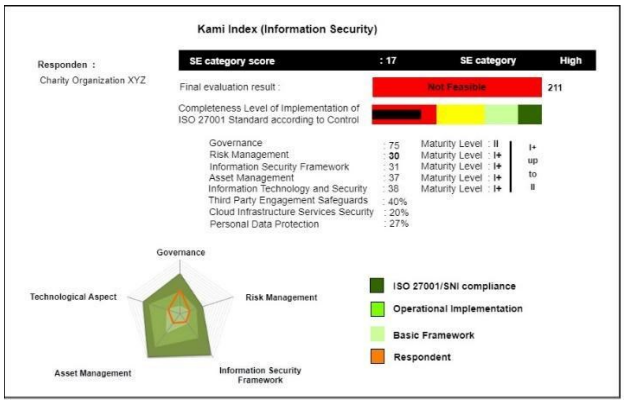

Fig. 4. Dashboard KAMI Index 4.1.

A. Electronic System Category

The electronic system category is the first category in the evaluation. The electronic system category evaluates the importance of using electronic systems in the budgeting system. The results of the assessment of the importance of the use of Electronic Systems in the budgeting system get score of 17, so that it can be included in the "High" category according to the guide table for the assessment of the electronic system category in TABLE I. the "High" category ranges from a score of 16 to 34. The total score for the electronic system category on the budgeting system can be seen in the dashboard of the KAMI Index 4.1 in Fig. 4.

B. Information Security Governance Category

The category of information security governance is an evaluation that can affect data on the budgeting system. Assessment of Information Security Governance in the budgeting system at Organization XYZ obtained a total evaluation score at 75 out of 22 questions with maturity level II status (Implementation of the basic framework). The expected maturity level for the minimum threshold for certification readiness is Level III+. Still, the results of Information Security Governance are only at maturity level II, which means that they are already implementing the basic framework. The evaluation results of information security governance are shown in Table III.

C. Information Security Risk Management Category

The information security risk category evaluates the management of information security risk, including various risks that can occur and affect information data on the budgeting system. Assessment of Information Security Risk Management on the budgeting system obtained a total evaluation value at score 30 out of 16 questions with maturity level status I+ (Initial Condition). The expected maturity level for the minimum certification readiness threshold is Level III+. However, this results are only at maturity level I+. The evaluation results are shown in Table IV.

TABLE III
INFORMATION SECURITY GOVERNANCE EVALUATION

Security Status	Maturity Level						Total
	1	score	2	score	3	score	
Not done	0	0	0	0	0	0	0
In Planning	1	0	2	0	3	0	0
In progress	2	10	4	20	6	18	48
Fully applied	3	9	6	18	9	0	27
Total Score							**75**

TABLE IV
INFORMATION SECURITY RISK MANAGEMENT EVALUATION

Security Status	Maturity Level						Total
	1	score	2	score	3	score	
Not done	0	0	0	0	0	0	0
In Planning	1	2	2	2	3	0	4
In progress	2	16	4	4	6	0	20
Fully applied	3	0	6	6	9	0	6
Total Score							**30**

D. Information Security Framework Category

Assessment of the Information Security Framework on the budgeting system obtained a total evaluation value of the Information Security Framework at score 31 out of 29 questions with a maturity level status of I+ (Initial Condition). The expected maturity level for the minimum certification readiness threshold is Level III+. However, the Information Security Framework results are only at

maturity level I+. The evaluation results are shown in Table V.

E. Asset Management Category

Assessment of Information Security Asset Management on the budgeting system at Organization XYZ obtained an evaluation of Information Security Asset Management of 37 out of 38 questions with maturity level status I+ (Initial Condition). The expected maturity level for the minimum certification readiness threshold is Level III+. However, the Information Security Asset Management result is only at maturity level I+. The evaluation results of information security governance are shown in Table VI.

TABLE V
INFORMATION SECURITY FRAMEWORK EVALUATION

Security Status	Maturity Level						Total
	1	score	2	score	3	score	
Not done	0	0	0	0	0	0	0
In Planning	1	4	2	6	3	0	10
In progress	2	4	4	8	6	0	12
Fully applied	3	9	6	0	9	0	9
Total Score							**31**

TABLE VI
ASSET MANAGEMENT EVALUATION RESULTS

Security Status	Maturity Level						Total
	1	score	2	score	3	score	
Not done	0	0	0	0	0	0	0
In Planning	1	6	2	2	3	0	8
In progress	2	14	4	12	6	0	26
Fully applied	3	3	6	0	9	0	3
Total Score							**37**

F. Category Information Technology and Security

Assessment of Information Security Technology Aspects on the budgeting system obtained score at 38 out of 26 questions, with maturity level status I+ (Initial Condition). The evaluation results of information security governance are shown in Table VII.

TABLE VII
THE RESULTS OF THE EVALUATION OF TECHNOLOGY AND INFORMATION SECURITY

Security Status	Maturity Level						Total
	1	score	2	score	3	score	
Not done	0	0	0	0	0	0	0
In Planning	1	1	2	0	3	0	1
In progress	2	14	4	8	6	0	22
Fully applied	3	3	6	12	9	0	15
Total Score							**38**

G. Supplement Category

The evaluation results at the supplement stage obtained that the maturity level for securing third-party involvement was 40%. Then for the security of cloud infrastructure services by 20% and the last is personal data protection by 27%.

V. CONCLUSION

Based on the results of the evaluation conducted on the level of readiness (completeness and maturity) of information security by using KAMI Index on the budgeting system in Organization XYZ, it can be concluded that: The Electronic System Area got a score of 17, so it was included in the high category; From the five observed information security areas, it is seen that they have better governance aspects compared to other information security areas (close to certification standards); Framework Area (31<36), Asset Management Area (37<72), and Technology Aspect Area (38<42), giving the results do not meet the basic framework. So, they have to improve somo aspect of information security policy; Of the five information security areas (Information Security Governance, Information Security Risk Management, Information Security Framework, Asset Management, and Technology), a total score of 211 is obtained. Based on the correlation with the Electronic System Category in TABLE I, 211 is between 0-272. Based on Fig 2, the level of completeness of information system security has a readiness status of "Not Feasible."; The minimum limit that must be achieved to be able to carry out ISO 27001 certification is III+. For now, the maturity level of the Work Unit of the Central XYZ Organization in the budgeting system is only limited to I+ to II. The information system security level is at the level of "Implementation of the Basic Framework."

ACKNOWLEDGEMENT

Thank you to Lembaga Penelitian dan Pengabdian Masyarakat (LPPM) Universitas Ahmad Dahlan who have provided funding for this research activity through Skema Penelitian Unggulan Program Studi (PUPS) in 2021 based on contract number PUPS-278/SP3/LPPM-UAD/VI/2021.

REFERENCES

[1] E. R. Pratama, Suprapto, and A. R. Perdanakusuma, "Evaluasi Tata Kelola Sistem Keamanan Teknologi Informasi Menggunakan Indeks KAMI dan ISO 27001: Studi Kasus KOMINFO Provinsi Jawa Timur," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 2, no. 11, pp. 5911–5920, 2018.

[2] T. Effendy *et al.*, "Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Kami) Pada Kantor Wilayah Kementerian Hukum Dan Ham Diy," vol. 3, no. 1, pp. 1–6, 2020.

[3] B. Sutara, "Pengukuran Keamanan Informasi PDAM Titra Medal Menggunakan Indeks KAMI Untuk Analisis Tingkat Kematangan Keamanan Informasi," vol. 17, no. 2, pp. 34–41, 2018.

[4] Yustanti, W. Rahadian, B. Anita, Q. Prihanto, and Agus, "Analisis Tingkat Kesiapan Dan Kematangan Implementasi Iso 27001 : 2013 Menggunakan Indeks Keamanan Informasi 3 : 2015 Pada UPT PPTI Universitas Negeri Surabaya" *Informatika,* vol 5, no. 4, pp. 1602–1613, 2016.

[5] M. R. Slamet, F. Wulandari, and D. Amalia, "Penilaian Pengamanan Teknologi Pada Sistem Pembelajaran Elektronik Menggunakan Indeks Keamanan Informasi Di Politeknik Negeri Batam," *Journal of Applied Business Administration*, vol. 3, no. 1, pp. 162–171, 2019, doi: 10.30871/jaba.v3i1.1305.

[6] W. W. W. S. Haries Anom Suseyto Aji Nugroho, "Metode Silogisme and Untuk Validitas Jawaban Dari Responden

Dalam Analisis Maturity Level Keamanan Informasi Berbasis Sni Iso 27001:2013 Pada Dinas Kependudukan Dan Pencatatan Sipil Kota Xyz," *Jurnal Transformasi*, vol. 14, no. 2, 2019.
[7] J. F. Andry and A. K. Setiawan, "It Governance Evaluation Using Cobit 5 Framework on the National Library," *Jurnal Sistem Informasi*, vol. 15, no. 1, pp. 10–17, 2019, doi: 10.21609/jsi.v15i1.790.
[8] Y. Sekhara, H. Medromi, and H. Nahla, "Multi Agent Decision system for the IT Governance Platform," vol. 15, no. 5, pp. 290–306, 2017.
[9] A. R. Riswaya, A. Sasongko, and A. Maulana, "Evaluasi Tata Kelola Keamanan Teknologi Informasi Menggunakan Indeks Kami Untuk Persiapan Standar Sni Iso/Iec 27001 (Studi Kasus: Stmik Mardira Indonesia)," *Jurnal Computech & Bisnis, Vol. 14, No. 1, Juni 2020, 10-18 ISSN (print): 1978-9629, ISSN (online): 2442-4943*, vol. 14, no. 1, pp. 10–18, 2020.
[10] N. A. Widodo and and A. F. R. , R. Rizal Isnanto, "Perencanaan Dan Implementasi Sistem Manajemen Keamanan Informasi Berdasarkan Standar ISO/IEC 27001:2005 (Studi Kasus Pada Sebuah Bank Swasta Nasional)," vol. 4, no. 1, pp. 60–66, 2016.
[11] N. E. Wowor *et al.*, "Analisa Keamanan Informasi Pemerintah Kota Manado Menggunakan Indeks Kami," *Jurnal Teknik Informatika*, vol. 13, no. 3, pp. 1–10, 2018, doi: 10.35793/jti.13.3.2018.28081.
[12] T. Hartati, "Perencanaan Sistem Manajemen Keamanan Informasi Bidang Akademik Menggunakan ISO 27001: 2013," *KOPERTIP : Jurnal Ilmiah Manajemen Informatika dan Komputer*, vol. 1, no. 2, pp. 63–70, 2017, doi: 10.32485/kopertip.v1i02.24.
[13] F. Febrianto and D. I. Sensuse, "Evaluasi keamanan informasi menggunakan ISO / IEC 27002 : studi kasus pada Stimik Tunas Bangsa Banjarnegara," *Infokam*, vol. 2, no. 2013, pp. 21–27, 2017.
[14] F. R. Industri and U. Telkom, "1) Pendahuluan," vol. 8, no. 2, pp. 2663–2677, 2021.
[15] N. Matondang, I. N. Isnainiyah, and A. Muliawatic, "Analisis Manajemen Risiko Keamanan Data Sistem Informasi (Studi Kasus: RSUD XYZ)," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 2, no. 1, pp. 282–287, 2018, doi: 10.29207/resti.v2i1.96.
[16] W. Apriandari and A. Sasongko, "Analisis Sistem Manajemen Keamanan Informasi Menggunakan Sni Iso / Iec 27001 : 2013 Pada Pemerintahan Daerah Kota Sukabumi (Studi Kasus : Di Diskominfo Kota Sukabumi)," *Ilmiah SANTIKA*, vol. 8, no. 1, pp. 715–729, 2018.
[17] R. Adi, P. Pratama, R. Sengkey, and C. Punusingon, "Analisis Keamanan Informasi Pemerintah Kabupaten Minahasa Tenggara Menggunakan Indeks KAMI," vol. 15, no. 3, pp. 189–198, 2020.
[18] B. A. Firzah, "Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Kami) Berdasarkan Iso / Iec 27001 : 2013 Pada Direktorat Pengembangan Teknologi Dan Sistem Informasi (Dptsi) Its Surabaya Evaluating Information Security Management Using Ind," vol. 6, no. 1, 2017.
[19] H. Hambali and P. Musa, "Analysis of Governance Security Management Information System Using Index Kami in Central Government Institution," *Angkasa: Jurnal Ilmiah Bidang Teknologi*, vol. 12, no. 1, 2020, doi: 10.28989/angkasa.v12i1.563.
[20] M. Bakri and N. Irmayana, "Analisis Dan Penerapan Sistem Manajemen Keamanan Informasi Simhp Bpkp Menggunakan Standar Iso 27001," *Jurnal Tekno Kompak*, vol. 11, no. 2, p. 41, 2017, doi: 10.33365/jtk.v11i2.162.
[21] M. Lenawati, W. W. Winarno, and A. Amborowati, "Tata Kelola Keamanan Informasi pada PDAM Menggunakan ISO/IEC 27001:2013 dan COBIT 5," *Sentra Penelitian Engineering dan Edukasi*, vol. 9, no. 1, pp. 44–49, 2017.
[22] Y. C. Pradipta, Y. Rahardja, M. N. N. Sitokdana, U. Kristen, and S. Wacana, "Teknologi Informasi Dan Komunikasi Penerbangan Dan Antariksa (Pustikpan) Menggunakan Sni Iso / Iec 27001 : 2013," pp. 352–358, 2013.
[23] W. C. Pamungkas and F. T. Saputra, "Evaluasi Keamanan Informasi Pada SMA N 1 Sentolo Berdasarkan Indeks Keamanan Informasi (KAMI) ISO/IEC 27001:2013," *Jurnal Sistem Komputer dan Informatika (JSON)*, vol. 1, no. 2, p. 101, 2020, doi: 10.30865/json.v1i2.1924.
[24] Aucla, "No TitleΕΛΕΝΗ," *Αγαη*, vol. 8, no. 5, p. 55, 2019.
[25] BSSN, "Indeks Keamanan Informasi (Kami)," *Badan Siber dan Sandi Negara (BSSN)*, no. November, 2019.

Tawar is an alumni of the Gadjah Mada University Computer Science Study Program, both undergraduate and postgraduate. Currently working as a lecturer at the Information Systems Department of Ahmad Dahlan University, Indonesia. He previously served as Head of the Bureau of Information and Communication systems (2008–2020). Currently, he is the Head of Data and Information Center Development. He has research interests in e-governance and information technology governance.

Dr. Imam Riadi is an alumnus of Electrical Engineering Education, Yogyakarta State University for undergraduate degree, and Computer Science, Gadjah Mada University for master and doctorate degree. Currently working as a lecturer at the Information Systems Study Program and Masters in Informatics, Ahmad Dahlan University, Yogyakarta, Indonesia.

Adiniah Gustika Pratiwi was born in Metro, Lampung on August 26, 2000. She is a 2018 student at the Information Systems Department, Ahmad Dahlan University. He has also attended an internship program at Technophoria Indonesia.

Ariqah Adliana Siregar was born in Medan May 12, 2000. She is a 2018 student majoring in Information Systems, Ahmad Dahlan University. He was a member of the Student Executive Board of the Faculty of Applied Science and Technology. He has also participated in an internship at the SI-UAD Expression Room.