Analysis and Development of Information Security Framework for Distributed E-Procurement System

Sugianto
Department of Electrical Engineering
Universitas Indonesia
Jakarta, Indonesia
sugianto 71@ui.ac.id

Muhammad Salman
Department of Electrical Engineering
Universitas Indonesia
Jakarta, Indonesia
muhammad.salman@ui.ac.id

Yohan Suryanto
Department of Electrical Engineering
Universitas Indonesia
Jakarta, Indonesia
yohan.suryanto@ui.ac.id

***Abstract*—This paper proposes an information security framework for distributed E-Procurement system in Indonesia. E-Procurement in Indonesia has been implemented since 2008, and has provided many benefits. However, there are also information security issues in the use of IT. Developing an information security program is needed to overcome the issues. We compare and analyze the LPSE and ISO 27001 Standards to develop framework. The results show there are some gaps between LPSE Standard and ISO 27001. By implementing the proposed framework, LPSE as a provider of distributed E-Procurement system can be easier to implement the LPSE and ISO 27001 Standards simultaneously as an obligation to comply with government regulations.**

Keywords—Information Security, Framework, Distributed E-Procurement, LPSE Standard, ISO 27001

I. INTRODUCTION

In Indonesia, electronic public procurement (E-Procurement) has been implemented since 2008. Unlike in most countries that implement a centralized E-Procurement system, the implementation strategy of E-procurement in Indonesia use centralized and distributed system. The centralized system is managed by National Public Procurement Agency (LKPP), while the distributed system is managed by LKPP and E-Procurement Services Agency (LPSE).

The implementation of E-Procurement in Indonesia has provided many benefits to the government and suppliers. Suppliers can save costs for transportation, accommodation, consolidation and printing documents. For the government, the implementation of E-Procurement has a positive and significant influence on the absorption of the budget [1], and on procurement performance [2]. The implementation of E-Procurement also have influence in suppressing or preventing fraud [3], [4].

In addition to providing benefits, there are information security issues in the use of information technology. Zainuri et al conducted a risk assessment on the LPSE of Yogyakarta Province, the results showed that there was a high risk in the information technology attack category [5]. They recommend to implement information security standards. Huda et al conducted research to look for potential fraudulent practices in the implementation of E-Procurement in Indonesia. The results show that there are 2 categories of potential fraud, insider fraud and outsider fraud [6]. Insider fraud comes from internal personnel such as internet network (bandwidth) restrictions, firewall device configuration interventions, and changing or deleting files. Whereas fraud outsider comes from outside such as hacking, intrusion, and former system administrators who feel disappointed.

Developing an information security program is needed to avoid the threats. There are several components in developing information security, and one of the component is framework [7]. LKPP as the supervisor of the implementation of E-Procurement in Indonesia has developed and implemented a Standard which is a framework for assessing and evaluating the services, capacity and information security held by LPSE. This standard is listed in the Head of LKPP Regulation Number 9 of 2015 concerning E-Procurement Services Improvement. The government through the Ministry of Communication and Information has also issued the Minister of Communication and Information Regulation Number 4 of 2016 concerning Information Security Management System which requires electronic system operators to implement a standard security information management system based on ISO 27001. It means, LPSE is required to apply those 2 Standards, LPSE Standard and ISO 27001. Based on the efforts of LKPP and Minister of Communication and Information in improving information security on LPSE, it is necessary to analyze the implementation of these two standards so does not to overlap each other and avoid the implementation of information security repeatedly.

This research focuses on analysis and development a framework of information security for LPSE as a provider of distributed E-Procurement system. The proposed framework in this research is based on the LPSE and ISO 27001 Standards. Several interesting studies have been conducted about developing information security framework based on ISO 27001. Achmadi et al propose an Information Security Management System (ISMS) framework that is specific to Data Centers [8]. Rutanaji et al conduct research on the governance of digital archive information security based on cloud computing [9].

Several documents will be analyzed to find whether thera are gaps or not between the LPSE and ISO 27001 standards before proceeding with the new proposed framework. Then the proposed framework will be developed after it is known whether there are gaps or not. If there is no gap, it means that information security in the LPSE Standard is in accordance with ISO 27001. In other words when LPSE has implemented the LPSE Standard, it has also implemented ISO 27001. Section 2 introduces about E-Procurement in Indonesia, Information Security, LPSE Standard, and ISO 27001. Section 3 describes research methodology. Section 4 presents the results and discussion of information security framework

for distributed E-Procurement system. And the last section is the conclusion of this paper.

II. Literature Review

A. E-Procurement in Indonesia

E-Procurement has been implemented since 2008 in Indonesia. LKPP is the institution who responsible for E-Procurement implementation. Unlike in most countries that implement a centralized E-Procurement system such as Singapore, South Korea, Australia, Great Britain, Bangladesh, Turkey and India [10]–[14], the implementation strategy of E-procurement in Indonesia use centralized and distributed system [15]. Fig 1 shows an E-Procurement system architecture in Indonesia.

- E-Planning provides the procurement general plan of all government institutions in one year.
- The Vendor Selection System consists of several types of selection methods in procurement.
- E-Contract is a system to create a procurement contract document.
- E-Audit is a system for conducting audits of the procurement process.
- Vendor management system is a vendor data management system.
- INAPROC is a procurement portal that provides government procurement information in Indonesia.
- E-Monev is used to monitor and evaluate the government procurement processes.
- INAPROC Service Bus is a system for interconnection with other systems.

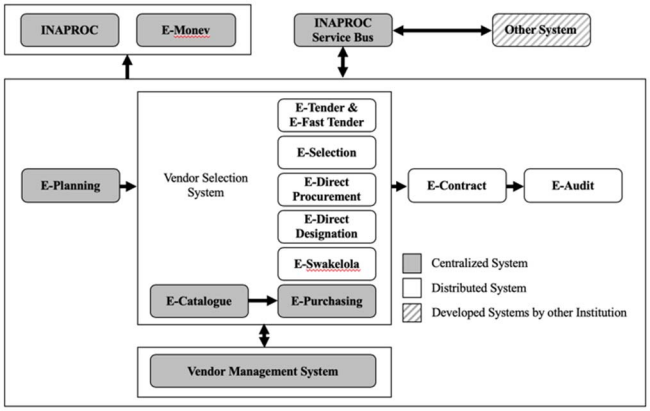

Fig 1. E-Procurement System Architecture

The centralized system is managed by LKPP, while the distributed system is managed by LKPP and LPSE. There are 694 LPSE who managed distributed E-Procurement system in Indonesia [16]. In the last 6 years, the average number of procurement packages per year is 138,000 packages, with an average value of 339 trillion per year, and savings of 28 trillion (10.4%) per year [17]. Table 1 shows transaction in the last 6 years. The number of registered users is more than 2.5 million, and the detailed of registered users shown in Table 2.

TABLE I. E-Procurement Transaction (Last 6 Years)

Description	2013	2014	2015	2016	2017	2018
Package (in thousand)	132	136	162	148	124	126
Value (in trillion)	249	310	318	399	396	359
Saving (in trillion)	22	21	25	28	36	37
Saving (%)	10.2	10.0	10.1	9.3	11.3	11.2

TABLE II. Registered Users

No	Users	Total
1.	Commitment Maker Officer	76.301
2.	Procurement Agent	241.966
3.	Procurement Officer	15.309
4.	Supplier	2.259.492
5.	Auditor	7.007

B. Information Security

Information security is the protection of information and critical elements, including systems and hardware that use, store and send information. Information security has 3 aspects, namely Confidentiality (C), Integrity (I), and Availability (A), known as the CIA [18]. Confidentiality: all information must be protected in accordance with the level of content privacy, so that only entitled people can access information. Integrity: all information must be stored under the same conditions when information is accessed by the owner. It means that the information is still intact and accurate, and that there are no intentional or accidental modifications from parties that do not have the right. Availability: all information which generated or obtained by the user must be available when needed. In other words, users can access information at any time without interruption.

The approach that can be taken to fulfill the aspect of information security is by building an information security program. Fig 2 shows the components of building an information security program [7]. One of the component is framework.

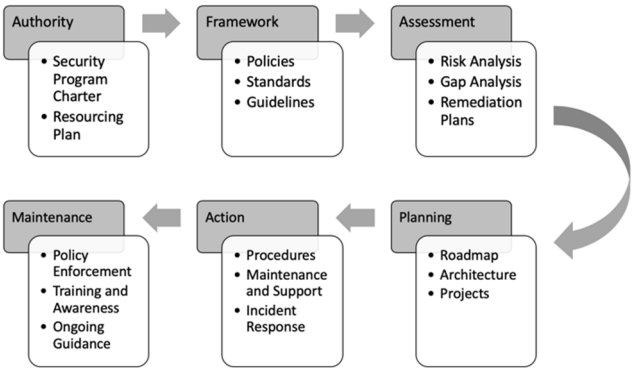

Fig 2. Security Program Components

C. LPSE Standards

The LPSE standard is a benchmark in written guidelines on various service processes for LPSE [19]. The purpose of implementing the LPSE Standard is to improve the quality of services, capacity and information security in the implementation of E-Procurement held by LPSE. There are 17 standards (Std Num 1 until Std Num 17) in the LPSE Standard shown in Table 3. The LPSE standard consists of 44 criteria that must be applied by LPSE.

TABLE III. LPSE STANDARD

Std Num	Standard
Std 1	Service Policy
Std 2	Service Organization
Std 3	Asset Management
Std 4	Risk Management
Std 5	Helpdesk Management
Std 6	Change Management
Std 7	Capacity Management
Std 8	Human Resource Management
Std 9	Device Security Management
Std 10	Operational Security Management
Std 11	Server and Network Security Management
Std 12	Continuity Management
Std 13	Budget Management
Std 14	Supplier Management
Std 15	Management of Relationship with Users
Std 16	Compliance Management
Std 17	Internal Assessment

D. ISO 27001

ISO 27001 which has the official name of the International Organization for Standardization/International Electrotechnical Commission 27001: 2013 (ISO/IEC 27001:2013) is an international standard focusing on Information Security Management Systems (ISMS). This standard is made to meet the needs starts from building, implementing, maintaining, and improving the information security management system. ISMS policy determination is based on a risk management approach, which begins with an understanding of the business environment and also evaluation of resources and processes to identify possible information security risks. After risk identification is carried out, the organization evaluates each risk and evaluates the potential impact that will occur, then makes a risk management strategy. The entire process requires extensive involvement from the management and officers (employees) who carry out the operation.

The ISO 27001 structure consists of 10 clauses and 114 controls that summarized in 14 control domains. The clauses contained in ISO 27001 are:

1. Scope
2. Normative references
3. Term and definition
4. Context of the organization
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance evaluation
10. Improvement

The control domains in ISO 27001 are contained in the Appendix A section, as shown in Table 4 [8].

TABLE IV. CONTROL DOMAIN IN ISO 27001

Annex	Domain	Control
A.5	Information security policies	2
A.6	Organization of information security	7
A.7	Human resource security	6
A.8	Asset management	10
A.9	Access Control	14
A.10	Cryptography	2
A.11	Physical and environmental security	15
A.12	Operations security	14
A.13	Communications security	7
A.14	System acquisition, development and maintenance	13
A.15	Supplier relationships	5
A.16	Information security incident management	7
A.17	Information security aspects of business continuity management	4
A.18	Information security revies	8

III. METHODOLOGY

This study uses literature information related to E-Procurement implementation in Indonesia, information security, LPSE Standard, and ISO 27001. The resources come from regulation, standard, journal, book, and the result of previously study. We compare the LPSE Standard and ISO 27001 Standard, then we look for the gaps between those of 2 standards. All those information is used as the basis for designing information security framework for LPSE as the distributed E-Procurement provider in Indonesia. The proposed framework will be merged with the LPSE Standard, so LPSE can implement those of 2 standards simultaneously as an obligation to comply with government regulations.

IV. INFORMATION SECURITY FRAMEWORK FOR DISTRIBUTED E-PROCUREMENT SYSTEM

In this section, we compare and analyze the LPSE Standard and ISO 27001 to find the related and the gap between criteria in Standard LPSE and control in ISO 27001. Then we classify each criteria and control to develop the proposed framework.

A. Gap between LPSE and ISO 27001 Standards

TABLE V. RELATED AND GAP CONTROL BETWEEN LPSE AND ISO 27001 STANDARDS

Std Num	Related Clause/Control	Gap Control
Std 1	A.5.1.1	A.5.1.2
Std 2	A.6.1.1	A.6.1.2
Std 3	A.8.1.1; A.8.1.2; A.8.2.1; A.8.2.2; A.8.2.3	A.8.1.3; A.8.1.4
Std 4	6.1.2, 6.1.3	-
Std 5	A.16.1.2; 1.16.1.6	A.16.1.4; A.16.1.5
Std 6	A.12.1.2; A.12.2.1	-
Std 7	A.12.1.3	-
Std 8	A.7.1; A.7.2; A.7.3	-
Std 9	A.11.1.3; A.9.1.1; A.8.3.2; A.6.2.1; A.8.3.1	A.8.3.3
Std 10	A.12.1.1; A.8.2.1; A.8.2.2; A.6.1.2; A.6.2.2	-
Std 11	A.9.1.1; A.9.1.2; A.13.1.1; A.12.3; A.12.4.1	-
Std 12	A.17.1.1; A.17.1.2; A.17.1.3	A.17.2.1
Std 13	-	-
Std 14	A.15.1.2	A.15.1.1
Std 15	-	-
Std 16	A.18.1.1; A.18.1.2	-
Std 17	A.18.2.1	A.18.2.3

We compare and mapping each criteria in LPSE Standard with control in ISO 27001. Based on the comparison and mapping between LPSE Standard and ISO 27001 Standard, in general, there are many criteria of LPSE Standard that are related with controls of ISO 27001. And we found some gaps as shown in Table V. Std Num is the Standard in LPSE Standard, Related Clause/Control is clause or control of ISO 27001 which found in LPSE Standard, and Gap is the gaps that we found which are controls of ISO 27001 that has not found in the LPSE Standard.

Detail of Related Clause/Control of ISO 27001 in LPSE Standard shown in Table 6, while detail of Gap Control shown in Table 7. In addition there are some criteria of LPSE Standard that not found in ISO 27001 as shown in Table 8. The Organization goal criteria in Std 2 not contained in ISO 27001, because the goal of organization not only describe related to the information security, but also to the capacity and service management.

TABLE VI. RELATED CLAUSE/CONTROL IN LPSE STANDARD

Std Num	Related Clause/ Control	Clause/Control Name
Std 1	A.5.1.1	Policies for information security
Std 2	A.6.1.1	Information security roles and responsibilities
Std 3	A.8.1.1	Inventory of assets
	A.8.1.2	Ownership of assets
	A.8.2.1	Classification of information
	A.8.2.2	Labelling of information
	A.8.2.3	Handling of assets
Std 4	6.1.2	Information security risk assessment
	6.1.3	Information security risk treatment
Std 5	A.16.1.2	Reporting information security events
	A.16.1.6	Learning from information security incidents
Std 6	A.12.1.2	Change management
	A.12.2.1	Controls against malware
Std 7	A.12.1.3	Capacity management
Std 8	A.7.1	Prior to employment
	A.7.2	During employment
	A.7.3	Termination and change of employment
Std 9	A.11.1.3	Securing offices, rooms and facilities
	A.9.1.1	Access control policy
	A.8.3.2	Disposal of media
	A.6.2.1	Mobile device policy
	A.8.3.1	Management of removable media
Std 10	A.12.1.1	Documented operating procedures
	A.8.2.1	Classification of information
	A.8.2.2	Labelling of information
	A.6.1.2	Segregation of duties
	A.6.2.2	Teleworking
Std 11	A.9.1.1	Access control policy
	A.9.1.2	Access to networks and network services
	A.13.1.1	Network controls
	A.12.3	Backup
	A.12.4.1	Event logging
Std 12	A.17.1.1	Planning information security continuity
	A.17.1.2	Implementing information security continuity
	A.17.1.3	Verify, review and evaluate information security continuity
Std 14	A.15.1.2	Addressing security within supplier agreements
Std 16	A.18.1.1	Identification of applicable legislation and contractual requirements
	A.18.1.2	Intellectual property rights
Std 17	A.18.2.1	Independent review of information security

TABLE VII. GAP OF CONTROL BETWEEN LPSE AND ISO 27001 STANDARDS

Std Num	Gap Control	Control Name
Std 1	A.5.1.2	Review of the policies for information security
Std 2	A.6.1.2	Segregation of duties
Std 3	A.8.1.3	Acceptable use of assets
	A.8.1.4	Return of assets
Std 5	A.16.1.4	Assessment of and decision on information security events
	A.16.1.5	Response to information security incidents
Std 9	A.8.3.3	Physical media transfer
Std 12	A.17.2.1	Availability of information processing facilities
Std 14	A.15.1.1	Information security policy for supplier relationships

TABLE VIII. GAP OF CRITERIA BETWEEN LPSE AND ISO 27001 STANDARDS

Std Num	Standard
Std 1	Public Policy
	Service Policy
Std 2	Organization Goal
Std 13	Identification of Service Needs
	Monitoring of Budged Usage
Std 15	User Satisfaction Survey
	Evaluation of User Satisfaction Survey

B. *Proposed Framework*

From previous works, we classify the criteria and controls contained in the LPSE and ISO 27001 Standard. The classification is made based on Table 6, 7, and 8. First, we classify the criteria which only contained in LPSE Standard (based on Table 8) as shown in Table 9. Second, we classify the criteria/control which contained in LPSE and ISO 27001 Standard (based on Table 6) as shown in Table 10. Third, we classify the control which contained in ISO 27001 (based on Table 7) as shown in Table 11.

TABLE IX. CRITERIA CONTAINED IN LPSE STANDAR

Std Num	Criteria	Classification
Std 1	-Public Policy -Service Policy	Public and Service Policies
Std 2	-Organization Goal	Organization Goal
Std 13	-Identification of Service Needs -Monitoring of Budged Usage	Budget Management
Std 15	-User Satisfaction Survey -Evaluation of User Satisfaction Survey	Management of Relationships with Users

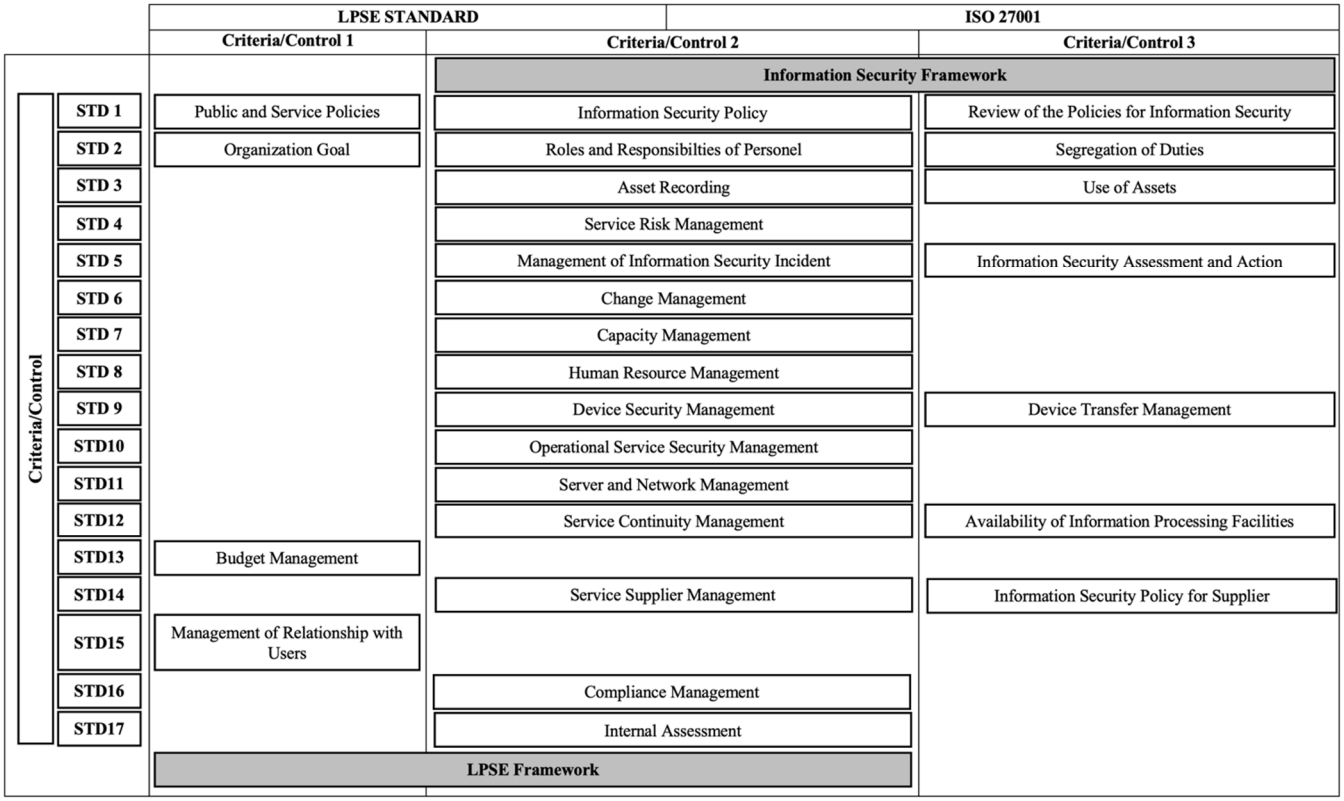

Fig 3. Information Security Framework for Distributed E-Procurement System

TABLE X. CRITERIA/CONTROL CONTAINED IN LPSE AND ISO 27001 STANDAR

Std Num	Criteria/ Control	Classification
Std 1	A.5.1.1	Information Security
Std 2	A.6.1.1	Roles and Responsibilities of Personnel
Std 3	A.8.1.1; A.8.1.2; A.8.2.1; A.8.2.2; A.8.2.3	Asset Recording
Std 4	6.1.2, 6.1.3	Service Risk Management
Std 5	A.16.1.2; A.16.1.6	Management of Information Security Incident
Std 6	A.12.1.2; A.12.2.1	Change Management
Std 7	A.12.1.3	Capacity Management
Std 8	A.7.1; A.7.2; A.7.3	Human Resources Management
Std 9	A.11.1.3; 1.9.1.1; A.8.3.2; A.6.2.1; A.8.3.1	Device Security Management
Std 10	A.12.1.1; A.8.2.1; A.8.2.2; A.6.1.2; A.6.2.2	Operational Service Security Management
Std 11	A.9.1.1; A.9.1.2; A.13.1.1; A.12.3; A.12.4.1	Server and Network Management
Std 12	A.17.1.1; A.17.1.2; A.17.1.3	Service Continuity Management
Std 14	A.15.1.2	Service Supplier Management
Std 16	A.18.1.1; A.18.1.2	Compliance Management
Std 17	A.18.2.1	Internal Assessment

TABLE XI. CONTROL CONTAINED IN ISO 27001

Std Num	Control	Classification
Std 3	A.8.1.3; A.8.1.4	Use of Assets
Std 5	A.16.1.4; A.16.1.5	Information Security Assessment and Action
Std 9	A.8.3.3	Device Transfer Management
Std 13	A.17.2.1	Availability Of Information Processing Facilities
Std 15	A.15.1.1	Information Security Policy For Service Supplier

Based on the classification, then we design the proposed framework. The proposed framework consists of an information security framework and LPSE framework for distributed E-Procurement system as shown in Fig 3. There are 3 categories of Criteria/Control classification based on LPSE and ISO 27001 Standards as follow:

- Criteria/Control 1: Criteria/control which contained in LPSE Standard
- Criteria/Control 2: Criteria/control which contained in LPSE and ISO 27001 Standard
- Criteria/Control 3: Criteria/control which contained in ISO 27001

We map the 3 categories of criteria/control classification with each standard which contained in LPSE Standard. So LPSE will more easier to implement both of those standards. For LPSE that has implemented all LPSE Standard (17 Standards), they can complete the Criteria/Control 3 which is the gap between LPSE and ISO 27001 Standard. So that information security at LPSE can be improved. For LPSE that

has not implemented part or all of the LPSE standards, they can apply the criteria/controls of the standards (Std 1 until Std 17) that needed or will be implemented first. So the implementation of the two standards does not overlap each other, and avoid the implementation of information security repeatedly.

V. CONCLUSION

Based on our works, the LPSE Standard has already comply with ISO 27001, although there are some gaps between both of those 2 standards. There are 2 clauses and 37 controls of ISO 27001 which related with LPSE Standard. While there are 9 controls of ISO 27001 which are the gaps between LPSE and ISO 27001 Standard. There are also 7 criteria of LPSE Standard that are not related to information security. There are even standards of LPSE Standard that are not related to information security (Std 13: Budget Management, and Std 15: User Relationship Management).

We developed an information security framework for distributed E-Procurement system in Indonesia. The proposed framework consists of 2 main areas, information security and LPSE are. The proposed framework can help LPSE to implement the LPSE and ISO 27001 Standards simultaneously as an obligation to comply with government regulations.

REFERENCES

[1] E. D. Rerung, H. Karamoy, and W. Pontoh, "Faktor-Faktor Yang Mempengaruhi Penyerapan Anggaran Belanja Pemerintah Daerah: Proses Pengadaan Barang/Jasa Di Kabupaten Bolaang Mongondow Selatan," *Goodwill*, vol. Vol. 8, no. No. 2, 2017.

[2] T. Aryati and L. Pangaribuan, "Analisis Pengaruh Implementasi e-Procurement dan Kompetensi Pegawai Terhadap Kinerja Pengadaan Barang dan Jasa Kementeria Keuangan," *J. Penelit. dan Karya Imliah Lemb. Penelit. Univ. Trisakti*, vol. Vol. 41, no. No. 1, 2019.

[3] R. S. Nugoroho, A. H. Wanto, and Trisnawati, "Pengaruh Implementasi Sistem Pengadaan Secara Elektronik (E-Procurement) Terhadap Fraud Pengadaan Barang/Jasa Pemerintah (Studi pada Satuan Kerja Perangkat Daerah Kabupaten Magetan," *J. Adm. Publik*, vol. Vol. 3, no. No. 11, pp. 1905–1911, 2015.

[4] L. P. R. M. Artantri, L. Handajani, and E. Pituringsih, "Peran E-Procurement Terhadap Pencegahan Fraud pada Pengadaan Barang/Jasa Pemerintah Daerah di Pulau Lombok," *J. Neo-Bis*, vol. Vol. 10, no. No. 1, 2016.

[5] M. Zainuri, L. E. Nugroho, and Widyawan, "Risk Assessment dalam Perancangan Business Continuity Plan-Studi Kasus : LPSE DIY," *Pros. Semin. Nas. ReTII ke-10*, 2015.

[6] S. N. Huda, N. Setiani, R. Pulungan, and E. Winarko, "Potential Fraudulent Behaviours in e-Procurement Implementation in Indonesia," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. Vol. 185, 2017.

[7] M. Rhodes-Ousley, *Information Security The Complet Reference, Second Edition*. 2013.

[8] D. Achmadi, Y. Suryanto, and K. Ramli, "On Developing Information Security Management System (ISMS) Framework for ISO 27001-based Data Center," *2018 Int. Work. Big Data Inf. Secur.*, pp. 149–157, 2018.

[9] D. Rutanaji, S. S. Kusumawardani, and W. W. Winarno, "Penggunaan Kerangka Kerja SNI ISO/IEC 27001:2013 untuk Implementasi Tata Kelola Keamanan Informasi Arsip Digital Pemerintah Berbasis Komputasi Awan (Arsip Nasional RI)," *Pros. Semin. Nas. GEOTIK*, 2018.

[10] S. A. I. Mahmood, "Public Procurement System and e-Government Implementation in Bangladesh: The Role of Publice Administration," *J. Public Adm. Policy Res.*, vol. Vol. 5, pp. 117–123, 2013.

[11] A. Nurmandi, S. Kim, A. Mardiansyah, Z. Qodir, and M. K. Dalari, "Re-Examined E-Procurement In Decentralized-Indonesia's Local Government Procurement System," 2014.

[12] F. Asa, "Komparasi Information Technology Procurement Policy di Pemerintahan," *J. Inform. Mulawarman*, vol. Vol. 12, no. 1, pp. 38–44, 2017.

[13] R. K. Shakya, *Digital Governance and E-Government Principles Applied to Public Procurement*. IGI Global, 2017.

[14] "About Central Public Procurement Portal," 2019. [Online]. Available: https://eprocure.gov.in/cppp/sites/default/files/eproc/CPPP_Overview.pdf. [Accessed: 07-Apr-2019].

[15] Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah, *Implementasi e-Procurement sebagai Inovasi Pelayanan Publik*. 2009.

[16] Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah, "LPSE," 2019. [Online]. Available: https://eproc.lkpp.go.id/lpse.

[17] Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah, "Status Transaksi E-Tendering LPSE," 2019. [Online]. Available: http://report-lpse.lkpp.go.id/v2/beranda.

[18] Rosmiati, I. Riadi, and Y. Prayudi, "A Maturity Level Framework for Measurement of Information Security Performance," *Int. J. Comput. Appl.*, vol. Vol. 141, 2016.

[19] Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah, *Peraturan Kepala Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah Nomor 9 Tahun 2015 tentang Peningkatan Layanan Pengadaan Secara Elektronik*. 2015.