Potential fraudulent behaviors in e-procurement implementation in Indonesia

S N Huda[1], N Setiani[1], R Pulungan[2] and E Winarko[2]

[1] Department of Informatics, Universitas Islam Indonesia, Yogyakarta, Indonesia
[2] Department of Computer Science and Electronics, Universitas Gadjah Mada, Yogyakarta, Indonesia

E-mail: sheila@uii.ac.id, novi.setiani@uii.ac.id, pulungan@ugm.ac.id, ewinarko@ugm.ac.id

Abstract. Corruptions in public procurement have occurred in various parts of the world, especially in developing countries. Implementation of SPSE (electronic procurement system) as the e-procurement system in Indonesia is based on the government's intentions towards clean and good governance by fighting corruption, collusion, and nepotism. Procurement in Indonesia is carried out through SPSE, which is developed by LKPP (Government Policy on Procurement of Goods/Services). Although this system has brought many positive effects, there are still found many practices of fraud occurring in the implementation of the system. In this paper, we try to identify these practices and then to systematically categorize and analyze them.

1. Introduction

Burton [1] argues that public procurement is a core instrument to achieve efficient management of public resources. It supports jobs and government services and can cover a variety of needs, ranging from stationery, furniture, temporary office staffs, to a very complex and high-cost projects, such as construction, aircrafts, and other various projects.

Corruptions in public procurement have occurred in various parts of the world, especially in developing countries. Corruptions have negative effects on various levels: local, regional, and national [2]. Above all, corruptions adversely affect the competence of public and prosperity in a country, increase the cost of government operations and social structures, undermine confidence in the government, and unbalance the composition of government spending on a wide range of services, including education, health, operation, and maintenance. Thus, corruption is a lethal socio-economic problem, and unfortunately, is widespread in developing countries like Indonesia.

Sistem Pengadaan Secara Elektronik (electronic procurement system, abbreviated SPSE in Indonesian) is the decentralized e-procurement system of Indonesia developed by LKPP (Policy Institute for Government Procurement of Goods/Services). SPSE is run by LPSEs (Electronic Procurement Services). Now the number of LPSEs has reached 635, where the process of growing the number of LPSEs is a process that takes time and effort. It mainly depends on the political will of the local governments and on the awareness of the needs to implement e-procurement.

Implementation of SPSE is based on the government's intentions towards clean and good governance by fighting corruption, collusion, and nepotism. Corrupt practices are known to always occur in the practices of government procurements of goods and services [3]. According to a survey conducted by Indonesian Corruption Watch (ICW), which was presented to the Corruption Eradication Commission (KPK) in March 2011, 89% of companies supplying goods and services to the government had bribed to win tender offers [4]. On the other hand, companies making efforts (trying) to offer bribes reached 92%. The survey was conducted on 792 providers of goods and services in Jakarta, Bekasi, Tangerang, Depok, and Bogor [4]. ICW also reported that there are other corrupt practices in the procurement process of goods and services, which include 48 cases of mark-ups, 50 cases of illicit letters, 1 case of breach of contract, and 8 cases of false procurement projects [5].

The presidential decree No. 54 of 2010 states that e-procurement should be applied starting in 2012. The implementation of e-procurement is expected to reduce corruption because all processes of procurement tender are conducted online using the Internet, and thereby reducing the possibility of direct meetings between potential suppliers and procurement organizers.

In general, the implementation of e-procurement in Indonesia brings significant positive results [3]. Among the positive impacts of the implementation of e-procurement in Indonesia is increasing the efficiency of fund procurement, and increasing procurement transparency to reduce corrupt practices in order to achieve clean and good governance. However, few researches investigate frauds in the implementation of e-procurement itself. Although it has brought many positive effects, there are still found practices of fraud occurring in the implementation of e-procurement. For example, as disclosed by the head of LKPP, Agus Rahardjo, in 2014, LPSEs of Malang, Banten and Palembang have been given warning letters from LKPP citing deliberate intentions to block some companies or providers from getting into the tender process of procurement programs, so the winner of the tender process is some preferred or targeted partner company (http://www.lkpp.go.id/v3/#/read/2869, 25 September 2014).

Nurmandi [6] suggests that the status of e-procurement in Indonesia is in the middle of the status quo where until 2012 the number of procurements auctioned electronically by the central government only reached 10.26% of the total procurements and 21.10% of the total procurements are by local governments. Based on LPSE smart report in 2015 for 6 years of SPSE implementation, the total number of LPSEs increases from 10 with 33 total tender offers in the initial year to 570 LPSEs with 135.669 total tender offers and 129.728 finished tenders. These LPSEs rendered the tender processes more efficient by more than 17.9 billion Rupiahs, which is equivalent to 8.41% of the total budget.

Although the implementation of e-procurement has improved the transparency of the procurement process, some people are still able to exploit limitations of the system, and this in turn still allows for corrupt practices to occur. This paper discusses potential fraudulent behaviors that have occurred in the implementation of e-procurement in Indonesia.

2. Methodology

The method used in this paper is a qualitative research method with the primary method is to obtain data through interviews. Parties who were interviewed in the study include LKPP, several LPSEs, and providers of goods and services that have followed the tender process via e-procurement. Data collection was performed using purposive sampling, *i.e.*, by selecting individuals who have the expected data. We interviewed LKPP, provincial, district, and state higher education institution LPSEs, as well as providers of goods and services. After obtaining qualitative data, we analyze data using open coding thematic analysis method. Interview results will be identified as themes of occurred fraud cases that potentially threaten the implementation of e-procurement.

3. Potential fraudulent behaviors

Frauds in the e-procurement application can be categorized into behaviors that involve people from inside and outside of an LPSE. These behaviors are summarized in table 1.

Table 1. Insider Frauds and Outsider Attacks.

Insider

No.	Fraud	Common Cause
1	Bandwidth limitation	No systematic monitoring; Diverse security levels of decentralized LPSE servers; Lack of personnel's integrity.
2	Firewall rule intervention	
3	File changes/removals by system admins	
4	Subjectivity on assessment	

Outsider

No.	Attack	Common Cause
1	Hacking	Lack of security awareness; Diverse security levels of decentralized LPSE servers; Lack of personnel's integrity.
2	Instrusion	
3	Potentially dissatisfied ex-system admins	

3.1. Fraudulent behaviors by insiders

LKPP has issued standardizations for LPSEs whose components include availability, security and service. Security aspects are adopted from ISO 27001 with adjustments. These includes server placement in integrated data center, data center physical security, such as CCTV and finger print usage, recorded and limited access, and SSH regulation. However, this standardization is not mandatory for all LPSEs, resulting in a wide variation of LPSE server condition. Because of this variation of LPSE server condition, server security awareness also varies. Based on our research, several methods of frauds involve the procurement committees, including:

3.1.1. LPSE network/server bandwidth limitation This is usually done at the time of submission. At the time when the preferred provider has successfully input the bid file and all necessary documents have been uploaded 100%, server's bandwidth is reduced so that other potential providers are not able to upload their documents. Several LPSEs have been caught and given reprimands for committing a network cheat. The lure of cheating providers may attract system administrators with weak integrity.

On the other hand, government has to consider the welfare of the committees, especially system administrators, who hold great responsibility in managing e-procurement system. The welfare of system administrators, in the form of performance benefits, varies greatly among regions, depending on the LPSE position, along with the magnitude of the local budget. In LPSEs under Diskominfo (Government Office of Communications and Information Technology), their remuneration has been considered properly. But ad hoc LPSEs usually provide remuneration that is not as good as other areas. This can lead to a potential lack of integrity on the part of committees/system administrators, as they have similar workload between one region and others, but receive different remuneration. System administrators' quality is based on the aspects of skill, attitude, loyalty, and morale. In LPSEs located in a big city, it is easy to find system administrators with high skills. In remote areas, however, it is more difficult to find system administrators with good skills, let alone to filter their attitude, loyalty, and morale.

3.1.2. The use of firewalls to inhibit the tender process This is performed, for example, by creating a rule in an LPSE firewall, where key to the uploading document page is locked so that some providers' uploading document page is empty and potential providers therefore cannot upload their bidding documents. Network and firewalls are vulnerable because servers are managed by decentralized LPSEs.

In some LPSEs, distribution of roles exists to avoid network abuse. In East Java province's LPSE, for example, this role is divided into three institutions: the management of LPSE server in data center under the Office of Communications and Information Technology (Diskominfo) of East Java province, administration system under the Bureau of Development Administration, and UPT P2BJ as the tender committee. Hence, server management is not directly under the direct procurement committee. This restricts the tender committee from cheating on the network and firewall. Data center in Diskominfo of East Java province has met safety standards and the office expects each district/city in East Java province to put their LPSE servers in the provincial data center. However, there are many obstacles that make districts/cities reluctant to entrust their servers to the provincial data center. The sectoral ego between different government agencies is still high. Even with certified security standard ISO 27001 data center, some institutions are not willing to entrust their LPSE servers to the provincial data center.

For other cases, South Sumatra province's LPSE has been reprimanded for indications of frauds in the implementation of e-procurement several years ago. It became very difficult to restore public trust, so the LPSE chose to entrust its server to a competent and professional certified third party. This third party was also under direct supervision from LKPP, reducing potential misuse of the server and the network. However, this will relate to the dignity of government institutions, which in this case is Diskominfo as an institution that acts as the government's Chief Information Officer (CIO). This institution will be deemed incompetent to manage data center or LPSE server.

One solution to overcome the reluctance caused by sectoral ego and to restore the dignity of Diskominfo as CIO of government is to build data centers managed by Diskominfo, but to place them on a higher institution. For the province level, for instance, the server can be put in the governor's office, or for the district level, it can be put in the regents office, or other close location as long as it holds certified and standardized security. This requires a willingness from local leaders in order to minimize sectoral ego. On the other hand, LKPP actually has developed a program to record the activities of LPSE servers. But it is only limited to recording, and yet is not able to analyze the activity. The number of records obtained from 635 LPSEs is certainly very large, making analysis very difficult. So far, the record log is only used if there is a complaint so that research in this area is certainly required.

3.1.3. File changes by server administrators Changing files as well as the destruction or removal of files, such as bidding files, are intended to omit other potential providers' bidding documents, so that those potential providers will be void. The perpetrator will usually also erase the server access log. Moreover, some LPSEs have improper server rooms, in the sense that many people can access the server freely. Based on our research, some SKPDs (working units) put LPSE on a server that can be accessed by strangers, not physically safe, on the floor, or on a pile of boxes that are susceptible to physical damage. Even one LPSE put the server in the bidding room, where bidding room is accessible to just anyone, including potential providers who wish to upload bidding files locally. Not only physical damages, the risk of theft is also prominent.

3.1.4. Subjectivity in the assessment of technical and qualification evaluation During the evaluation of the bid proposal, price, qualification, and technical assessment are evaluated. For the evaluation of the price, since it is nominal, it can be ascertained objectively. However, for the qualification assessment and technical assessment, there is still a factor of subjectivity. For a single potential provider, one appraiser evaluation committee may assume that the provider has similar experience with the work being tendered, but it is also possibly judged as dissimilar by another committee; hence results in a minimum rate. Definition of similar or dissimilar yet is unclear. As another example, suppose there is a tender for an information system. It is currently possible that the appraiser of technical proposal has no background in information technology. Different backgrounds, such as economics and informatics, will have different way in assessing the technical proposal, resulting in valuations that are less objective.

3.2. Fraudulent behaviors by outsiders

3.2.1. Hacking by irresponsible people Some mischiefs from hackers, such as DDOS, malware, and backdoor, have occurred. Firewall setting is very important to prevent DDOS attacks. In some LPSEs DDOS attack did occur. The DDOS attack could be generally attacking the whole system in the domain (for example, attacking one district), or considered deliberately attacking only SPSE to impede the tender process, especially to make the system down and potential providers then cannot upload their bidding documents. In terms of data communication, since the SPSE application is a web-based application, it should use HTTPS (SSL) by default. From our observations, only about 20-30% of all existing LPSEs have taken advantage of the HTTPS protocol on their SPSE system. The rest, 70-80% of them, still use the HTTP protocol only [7].

3.2.2. Intrusion or infiltration Intrusion is performed by persons who are not permitted to gain administrator privileges. As reported in http://www.antaranews.com/berita/554513/bareskrim-usut-kasus-pembobolan-akses-lpse-kemen-pupr, and some other news portals, the intrusion problem had raised security problems in LPSEs. On infiltration, when permissions as system administrator is obtained, the perpetrator can change individual files, removing files, change the server's time, and so on. Disappearance of files has recently occurred in several LPSEs, which is caused by hackers who deliberately remove bidding files and leave only one file belonging to a partner provider who paid the hackers. It has been categorized as a criminal conduct and has been under criminal investigation.

3.2.3. Former system administrators System administrators who have resigned, or moved to other institutions, but still have access to the SPSE servers have a great opportunity to commit crimes. As an administrator who has access to the server, he can change or remove files. In various government agencies, there is no clear standard operating procedure for the mutation or resignation process of system administrators.

3.2.4. Information leakage Information leakage is basically not categorized as attack or fraud, but has potential to weaken SPSE. There is a very complete document standard operating procedure (SOP) of LPSEs published online. Some information from the SOP is information that should not be shared publicly, such as:

- SPSE installation process and detailed SPSE framework.
- Web configuration, path configuration, database configuration, and system/application log file.
- List of application packages and supporting applications, application paths and application versioning.
- Web security configuration, web application firewall usage, and other security modules.
- Database name, user and password used in training and production phase.
- Monitoring log instructions, data center safety, backup and recovery information.
- Security, infrastructure, and system incident handling procedures.

This information can be misused by hackers by making it easier for them to penetrate the SPSE security.

4. Conclusion and future work

Potential fraudulent behaviors in the implementation of SPSE can be categorized into two groups: frauds involving insiders and frauds in the form of attacks from outside. Computer system security can be divided into several layers: physical security layer, human resources (people) layer, data/communications engineering (system/technology) layer, and policy & procedure layer [8]. To handle human resources layer, the government needs to pay attention to the system or network administrators, to standardize their skills and remuneration. To handle physical security layer, government also needs to pay attention to the physical security of servers where the LPSE servers still have varied qualifications. The use of datacenter with high security standard needs to be done, at least in one province. Regencies/cities that have no adequate datacenter can entrust their LPSE servers to the province data center. Strengthening the security in technology layer, such as by cloud LPSEs, can be studied further. The last dimension, *i.e.*, the policy requires a study of information system management system (ISMS) implementation, which has been initiated by the Ministry of Communication and Information Technology, as soon as possible, considering that e-procurement is a strategic e-government service.

Acknowledgments

The authors would like to thank the Ministry of Research, Technology and Higher Education of Indonesia for funding this research.

References

[1] Burton R A 2005 Improving integrity in public procurement: the role of transparency and accountability *Fighting Corruption and Promoting Integrity in Public Procurement* (OECD Publishing) pp 23–8

[2] Ampratwum E F 2008 The fight against corruption and its implications for development in developing and transition economies *Journal of Money Laundering Control* **11** 76–87

[3] Setyadiharja R, Budiman S, Karim Z, Matridi R, Junriana J, Ferizone F and Nurmandi A 2014 E-procurement system technology: an analysis in electronic procurement service unit (LPSE) of Kepulauan Riau Province *The Asian Journal of Technology Management (AJTM)* **7** 93–107

[4] Kredibel 2011 E-procurement innovation towards free corruption procurement *Kredibel Procurement Magazine* **Oct.-Dec.** 12–3

[5] Purwanto A, Ibty I, Rofikah N and Indroyono P 2008 E-procurement in Indonesia (development services procurement electronic government) *Kemitraan Partnership dan LPSE Nasional*

[6] Nurmandi A 2013 What is the status of Indonesian e-procurement? *Journal of Government and Politics* **4** 350–73

[7] Sinambela J 2016 LPSE [in]security *Indonesia's Information Security Portal* URL `http://infosec.id/2016/05/lpse-insecurity/`

[8] Icove D, Seger K and VonStorch W R 1995 *Computer Crime: A Crimefighter's Handbook* (O'Reilly & Associates, Inc.)