Towards generalized process patterns for detecting corruption within the government using open data

Darusalam; Janssen, Marijn; Ubacht, Jolien

DOI
10.1145/3209281.3209282

Publication date
2018

Document Version
Final published version

Published in
Proceedings of the 19th Annual International Conference on Digital Government Research

Towards generalized process patterns for detecting corruption within the government using open data

Darusalam
Delft University of Technology
The Netherlands
d.darusalam@tudelft.nl

Marijn Janssen
Delft University of Technology
The Netherlands
m.f.w.h.a.janssen@tudelft.nl

Jolien Ubacht
Delft University of Technology
The Netherlands
j.ubacht@tudelft.nl

ABSTRACT

Governments are seeking for new ways to fight corruption within their own administration. The opening of data has the potential to involve citizens in detecting corruption by providing them the ability to view and analyze data about what is happening within the government. However, how open data can be used to detect corruption is not clear. In this paper general patterns for detecting corruption using open data are derived. The patterns are derived by analyzing a case study of e-Procurement at the local government level in Indonesia. E-procurement activities and the corresponding audit activities were analyzed. The following patterns for detecting corruption using open data were derived; 1) storing and opening documents, 2) cross-data comparison, 3) four-eyes-principles, 4) segregation of duties, 5) authorization, and 6) publishing application controls. Data about the activities and structure of the administrative processes should be opened to allow the public to scrutinize whether the process has implemented preventive and detective controls following the process patterns derived in this research. Furthermore, data should be opened about all phases of the administrative processes to enable the involvement of the public and use their 'many eyes' for detecting corruption.

CSS CONCEPTS

• **Information systems** → Information systems applications

KEYWORDS

Open Data, Corruption, e-Government, e-Procurement, patterns, process patterns, internal control, citizen participation

ACM Reference Format

Darusalam, M. Janssen, J. Ubacht. 2018. *Towards generalized process patterns for detecting corruption within the government using open data*. In Proceedings of 19th Annual International Conference on Digital Government Research (dg.o'18), Anneke Zuiderwijk and Charles C. Hinnant (Eds.). ACM, New York, NY, USA, 6 pages.

dg.o '18, May 30-June 1, 2018, Delft, Netherlands

ACM ISBN 978-1-4503-6526-0/18/05…$15.00
https://doi.org/10.1145/3209281.3209282

1 INTRODUCTION

Corruption is a well-known problem within the government and is not easy to deal with [7]. Corruption can be viewed as a "behavior which deviates from the normal duties of a public role because of private-regarding (family, close private clique) pecuniary or status gains: or violates rules against the exercise of certain types of private-regarding influences" [12, p. 4]. Corruption refers to behavior, "such as bribery (use of reward to pervert the judgments of a person in a position of trust), nepotism (bestowal of patronage because of ascriptive relation rather than merit), and misappropriation (illegal appropriation of public resources for private-regarding uses" [12, p. 4]. An additional problem related to corruption is the misuse of power by public officers [7]. There are many factors that can lead to corruption in government [12]. Two main factors are "need driven", and "greed driven". A recent strategy to fight corruption is by opening government data [18]. One of the benefits of open data is the government can become more transparent and accountable [8]. Despite the potential of open data there is limited work on which data should be opened to detect corruption. The purpose of this article is to identify patterns of activities to detect corruption within the government using open data. Patterns have been used in many domains, for instance business, architecture, economic, software engineering and telecommunication [16]. Ambler [1] defines a pattern as "a general solution to a common problem, one from which a specific solution may be derived" (p. 4). Hagen and Gruhn [5] view a pattern as "proven processes which solve a frequently recurring problem in a pattern like way" (p. 1). Our research aim is to derive patterns to detect corruption by using open data. As there are no patterns available, an in-depth case study is investigated to derive patterns that can be used for detecting corruption. In further work these patterns will be generalized. In the next section, we discuss the literature background. Section three presents the research approach. Section four presents the case study. In Section five patterns for identifying corruption using open data are presented. Finally, we present the conclusions that we derived and formulate future research in section six.

2 LITERATURE REVIEW IN DETECTING CORRUPTION USING OPEN GOVERNMENT DATA

In this section we first present the anti-corruption cycle to understand how corruption is tackled. Thereafter we provide an overview of controls to avoid and to detect corruption, as found in the literature. Finally, we discuss the role of open data for fighting corruption.

2.1 Anti-corruption cycle

Fighting corruption is often driven by the anti-corruption cycle, which can be broadly divided into four stages: prevention, detection, investigation and sanction [11]. Countries have translated this cycle into institutional frameworks and put different emphasizes. For example, the UK has established a strong prevention process, whereas emphasis in the United States or Brazil is more focused on the enforcement phase [4]. However, all countries employ activities in all four stages of the anti-corruption cycle. Despite that organizational arrangements of governmental institutions are different, the anti-corruption cycle allows for identifying anti-corruption functions or activities [11]. The first stage, named *prevention*, concerns actions, mechanisms and tools that are aimed at reducing corruption and/or increase the barriers and costs of corruption. Potential actors involved in this stage are policy makers, politicians, parliamentarians, regulatory bodies, civil society organizations (CSO's), Auditors, Corruption Watch, Administrative Agencies and international agencies. The second phase *detection* refers to mechanisms and tools that identify and illicit behavior as a result of corruption. Possible stakeholders are policy implementers (government agencies and internal control bodies), CSO's, journalists, Corruption Eradication Commission, Audit Board, and oversight institutions (auditors, controllers, and Parliament). The *investigation* phase is the third phase and contains mechanisms and tools intended to expose and compile information about the illicit behavior detected and the parties involved. Typical stakeholders involved are CSO's, journalists, oversight institutions (auditors, comptrollers, and parliament), national and foreign prosecuting institutions. The final phase *sanction* refers to the consequences intended to prosecute, and include measures such as fines, disciplinary measures, civil remedies and other sanctions. Typical stakeholders involved are suspects (persons conducting corruption, or people under investigation for corruption), oversight institutions (auditors, controllers), national and foreign prosecuting institutions, judiciary, and asset recovery agencies. In this paper our aim is to support policy-makers in the prevention phase (phase 1) and to introduce measures to detect corruption (phase 2). We elaborate on the type of controls as found in the literature in the next subsection

2.2 Controls to prevent and detect corruption

Controls should be built into administrative processes to avoid and detect corruption. Controls are often investigated by auditors to verify if administrative processes have been executed correctly. The data collected by these controls can also be opened to enable the public to view this data and identify possible corruption. There are several types of controls to detect corruption. *Internal controls* are included in internal administrative processes of organizations to give reasonable assurance of the system to achieve the set goal [10]. The three functions of internal control are (1) preventive control (deter problems before they arise), (2) detective control (discover problems that are not prevented) and (3) corrected control (identify and correct the problem and recover from the errors) [10]. There are two general types of internal control, namely general and application controls [10].

(1) *General control:* these are implemented by management on the organization's control environment such as IT infrastructure, software acquisition, development and maintenance controls. Often the financial department is responsible for maintaining correct organizational procedures and for annual accounts.
(2) *Application control:* these are controls in the software to prevent, detect, and evaluate transaction errors and fraud. These controls are concerned with the accuracy, completeness, validity, and authorization of the data captured, entered, processed, stored, transmitted to other systems, and reported.

General types of control are the four-eyes-principles and segregation of duties [14]. The *four-eyes-principle* is a requirement that business decisions need to be actively conducted by at least two individuals (four eyes) [15]. These individuals check each other to avoid mistakes and to avoid that a single person can commit fraud without being noticed. *Segregation of duties* entails that a single person is not given too many duties or responsibilities [14]. For example, those who are executing transactions should be different from those who make the annual reports. In addition no single person should be able to control a single process. The implementation of controls determines the potential for fraud. Therefore we argue that it is important to open information about how the controls are implemented in the administrative processes. The controls that we reviewed in this section will be used to develop patterns for detecting fraud. But before that we look into the role of open and how this can strengthen the detection of corruption in governmental processes.

2.3 Open data for corruption detection

The opening of data about the internal functioning of the government can empower citizens to participate in control and monitoring of the government and can help to detect corruption. Open government is a multi-faceted policy aimed at improving the levels of transparency and accountability in public administration and to stimulate engagement by the public [2]. The underlying idea is that by providing access to information, citizens can participate in monitoring of the government and can help to detect corruption by analyzing the data. The willingness of public servants and politicians to contribute to the collection and opening of data might vary. Those who are conducting corruption have no incentive to share data that can be used to detect their activities. Other stakeholders take up different roles in the process and their willingness and interest might vary. Whereas these stakeholders contribute to the tackling of corruption, they may have different views on how to accomplish this.

- *Suspects and potential corrupters.*Those who might be corrupt are the main subject of this research. They want to hide their activities and might want to prevent disclosure of data or might manipulate data to avoid that their activities are detected. Those whose activities should become transparent by opening data might or might not conduct corruption.
- *Corruption watch.* This institution aims for creating an accountable, accessible, and responsive government. Corruption watch is involved in using ICT to detect corruption. ICT can reduce corruption by providing a low-cost online

platform to monitor the government as well as reducing the cost for collecting, distributing and accessing government information [2].

- *Auditors.* Auditors are the persons in institutions who have the responsibility to check the correctness of activities. These types of organizations check the activities of governments. An audit is the systematic process of objectively obtaining and evaluating evidence regarding assertions about economic activities and events to ascertain the degree of correspondence between the assertions and established criteria, and communicate the results to interested users [17].
- *Administrative Agencies.* These organizations offer executive administrative processes to provide services and to execute policies. Administrative agencies use resources for conducting their activities. In general, many persons are involved in these agencies.
- *Society.* The society consists of citizens who are highly diverse. Their level of education, their knowledge of and their interest in using open data varies. Most citizens will not use or are not able to use open data. Also their motivations vary. Only a few will be able to make use of open data for corruption detection.
- *Politicians.* Elected persons who represent citizens. Some of them might be corrupt or being suspect of corruption, whereas others are dedicated to fighting corruption.

Stakeholder interests can be contradicting. An obvious one is that corruption watch, inspections, and auditors want public organizations to be accountable, accessible, and responsive, whereas those who are corrupt do not want to be caught and want to hide their activities. Another one is that the opening of data might result in additional activities and consume resources and in this way adding to the bureaucracy, whereas money and resources are limited. The many stakeholders and their interests make this a complex playing field. As such, it is paramount to understand the activities of the stakeholders in the process in which the data is collected, processed, and opened.

3 RESEARCH APPROACH

The *purpose* of this article is to identify patterns of activities for detecting corruption within the government. As there is limited work in this area and we need to gain deep insight into the administrative processes we opted for conducting a single, in-depth case study. A case study allows in providing a deep understanding of the mechanisms and processes used to identify corruption. Yin [19] defines a case study as: "an empirical inquiry that investigates a contemporary phenomenon within its real life context, when the boundaries between phenomenon and context are not clearly evident" (p.12). In our case study we analyzed the e-procurement activities of the local government in Palembang South Sumatera Indonesia to identify patterns of activities to detect corruption and to show how open data can be used within these patterns. This case study was chosen due to the use of an e-procurement system called system electronic procurement services (LPSE). Procurement processes are sensitive to corruption, as a lot of money is involved and activities are vulnerable for mark-up, forgery of documents, bribes and embezzlement. The case study data is a mix of secondary data for which we analyzed various sources, including the official website and official documents. In addition primary data was used from prior research [9] and the own experiences of one of the authors.. To investigate the case study we first described the administrative processes using the Business Process Modelling Notation (BPMN). We opted for using this language as the resulting diagrams were easy to understand by the people involved in the case study. Next, the mechanisms for conducting corruption were analyzed. Each process step was investigated. This yielded a list of possible ways for conducting corruption. We derived seven patterns for detecting corruption using open data. This set of patterns can be used to detect corruption systems that are vulnerable to corruption.

4 SYSTEM ELECTRONIC PROCUREMENT SYSTEM (LPSE)

The local government in Palembang South Sumatera Indonesia uses the Systems Electronic Procurement Service (LPSE) for the procurement of government goods and services. The LPSE system has been introduced to improve the efficiency, effectiveness, quality, and transparency in the procurement of goods and services. This system links vendors and governments in Indonesia. LPSE is a unit formed across ministries and other institutions to maintain the services system of procurements of goods and services. This system facilitates procurement officers in carrying out the procurement of goods and services electronically. This system also provides services for the provider of goods and services who are domiciled in the territory of the LPSE concerned.

Figure 1 provides an overview of current activities for procurement which are supported by the LPSE system. The procurement starts by defining the needs, which is followed by publishing the Request for Quotation (RFQ). Next, suppliers receive the RFQ and develop their quotes. The supplier sends the quotes to government. Once the government has received the proposals, and the deadline has passed, the proposals are evaluated, supplier(s) will be selected, a final tender will be requested and the contract is signed. Thereafter follows the execution of the contract in which the products and services are delivered and paid. Finally, the delivered products and services can be evaluated. According to local government regulation, all the working units of local government must use the LPSE system. This prevents bypassing and the risks of fraud. All the working units are obliged to announce their planning, implementation and final result of their procurement processes via the LPSE system. As such, there is a huge potential for opening data. The types of data available in the LPSE system are as follows [9]:

- *Auction announcement:* The LPSE system provides an announcement about what types of procurement are available from working units in Palembang;
- *Information about system failure:* This system provides information such as if the packet cannot be generated, upload file failure, so the system can provide solutions;
- *Electronic Catalogue (EC):* This system provides detailed listings of vendor offerings. For example: description of products, prices, delivery time. This EC can be used by automated procurement systems;
- *Monitoring and online evaluation:* The system provides information about planning packets of procurements, financial

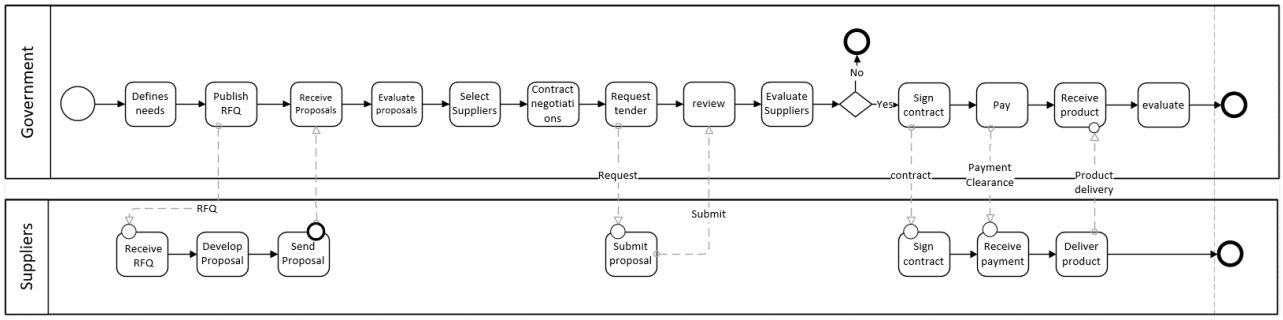

Figure 1: Overview of the e-procurement system

progress, physical progress, procurement goods and services progress;

- *Whistleblowing system:* The LPSE system has a link to https://wbs.lkpp.go.id/container.php. A person who has information about illegal or unethical activities or a suspicion of corruption related to procurement can use this link to report these activities to the corruption watch or audit board.

In the current system, there are all kinds of control mechanism, but currently there is no systematic policy to open the data that is generated within and by the system. In the next section we present patterns for detecting corruption using open data.

5 PATTERNS FOR DETECTING CORRUPTION

In this section, patterns will be described showing how open data can be used to detect corruption. In this research, we found six types of patterns for corruption detection, which are presented in table 1. These patterns will be discussed in detail in the next subsections.

#	Pattern name	Short description
1	Storing and opening documentation	Opening of documents generated in several activities
2	Cross-data comparison	Comparison of data collected in different phases to detect discrepancies
3	Four-eyes-principle	Opening of process information about decisions should be made by at least two independent persons
4	Segregations of Duties	Opening of process data to check whether a single individual or department is allowed to process a transaction in its entirety
5	Authorization	Opening of who is authorized to approve which activity
6	Application controls	Opening of data about built in measures to avoid the making of mistakes and the availability of alerts in the system

Table 1: Overview of patterns

5.1 Pattern: Storing and opening documentation

The documentation generated in several activities should be stored by an independent party and opened to the public. For instance the RFQ, minutes of meetings, received proposals, decisions, and payment must be opened to the public (see figure 2). The public can use these to check the correctness. These activities are stored into a repository that can be accessed by the public. Storing in a block chain or by an independent, trusted party avoids that the documents can be altered or manipulated. The immutable storing of data is a necessary basis for the other patterns (like for example the next pattern cross-data comparison).

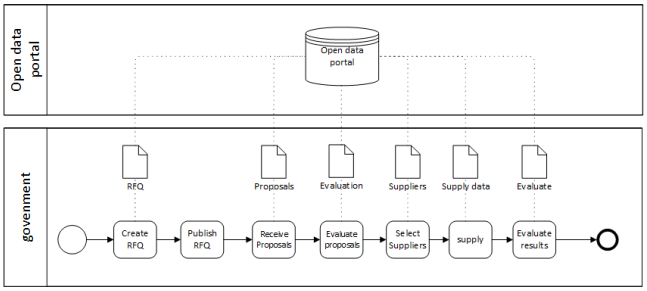

Figure 2: Pattern documentation

5.2 Pattern: Cross-data comparison

By comparing data collected at different phases of the e-procurement process, possible corruption might be detected. This pattern is schematically shown in Figure 3 in which the RFQ is compared with the results delivered. In this way the public or corruption watch is able to detect whether the requirements and needs stated in the RFQ are actually realized or whether there are any deviations.

The pattern shows that two sources of data can be used to compare with each other and can be applied in different areas in our case study, including the following:

(1) RFQs and the capabilities of the supplier selected
(2) Purchase orders and delivered goods/services
(3) Purchase orders and invoices
(4) Invoices and delivered goods/services
(5) Invoices and payment
(6) Selected vendors and project execution

By opening the data and comparing the results the public can scrutinize the various phases so society can detect any discrepancies between the planning and real execution.

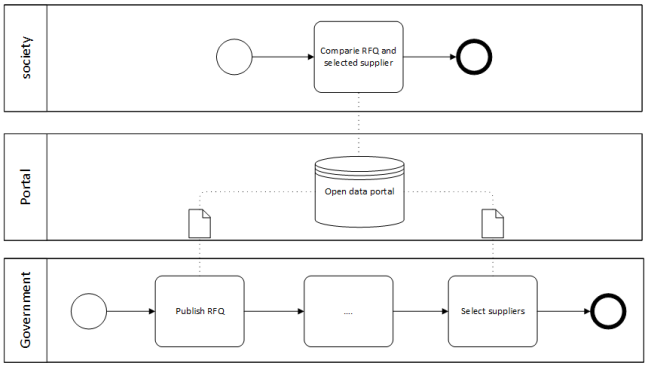

Figure 3: Pattern cross-data comparison

5.3 Pattern: Four-eyes-principle

One of the most effective controls to prevent corruption is application of the four-eyes-principle [13]. According to Schikora [15] the 'four-eyes-principle' is considered as one of the most potent measures against corruption although it lacks both theoretical and empirical justification. The four-eyes-principle in this case study in the system of LPSE procurement is that certain activities such as a decision, transaction, evaluation, and payment must be approved by at least two persons. This is expressed in Figure 4 by having two swim lanes; each referring to different responsibilities. Data about the different responsibilities can be opened, so the public can monitor and evaluate if the four-eye principles is (correctly) applied. The pattern four-eyes-principle is used to enable monitoring of the procurement process by the public. Checks can be done whether decisions are approved by a procurement committee (1st Approval) and an external auditor (2nd Approval).

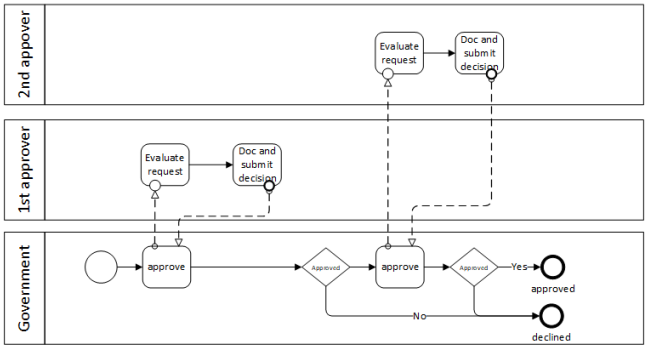

Figure 4: Pattern four-eyes-principle in publishing an RFQ

5.4 Pattern: Segregation of duties

Segregating of Duties is needed to ensure that no single individual or department processes a transaction in its entirety [6]. In our case there was no separation of certain duties between payment and accounting personnel in the LPSE system [3]. In addition, appropriation of separation of duties can ensure that accurate information is controlled by internal and external stakeholders as shown in figure 5.

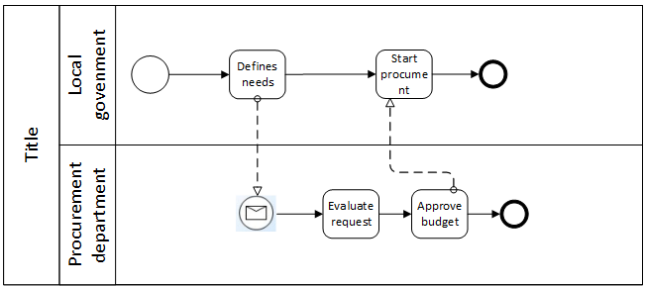

Figure 5: Pattern Segregation of duties

Segregation of duties is a type of preventive control [10]. In the pattern the definition of needs should be done by somebody else than the one who approves of the request in the second stage. This prevents that the same person checks his own actions, as illustrated in figure 6.

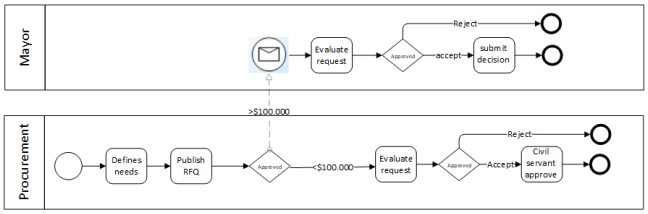

Figure 6: Pattern Authorization

5.5 Pattern: Authorization

The pattern Authorization refers to the need for having different levels of authorization. Often higher management layers approve decisions having more impact. Opening data about who is authorized for what can enable finding the person who might have conducted corruption. At least this serves as a preventive measure as decision-makers will be more reluctant to conduct fraud. The pattern authorization provides specifications for approval from the authorized person. For example, a procurement of more than >$100.000 must be approved by the major, however for procurements less than <$100,000 this is not necessary.

5.6 Pattern: Application controls

Application controls should prevent the making of mistakes, but they can also be used to detect errors and possible fraud (see figure 7). For example a simple control is that an invoice cannot be higher than the amount stated in the RFQ. In case the amount of multiple invoices goes above the agreed price, the system should send out an alert.

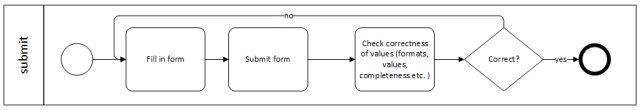

Figure 7: Pattern Application controls

An example of an application control in the system is that vendors have to complete all the fields on the screen before they can submit a form.

6 CONCLUSION AND FURTHER RESEARCH

The opening of data enables a move from a closed to an open system in which the public can become involved in detecting corruption. Based on our case study in which we analyzed the LPSE for the local government in Palembang South Sumatera Indonesia for the procurement of government goods and services, we derived six patterns for detecting corruption using open data: 1) storing and opening documents, 2) cross-data comparison, 3) four-eyes-principles, 4) segregation of duties, 5) authorization, and 6) publishing application controls. The patterns show that not only the data that is generated during the e-procurement process should be opened, but also information about the operation of the administrative processes and the implemented measures to prevent corruption.. The latter enables the design of processes that are better in preventing corruption. Based on our case study, we claim that data should be opened about decision-making activities in all phases of the e-procurement process to allow for the comparison of data among the steps. The public can be provided with insight into, for example, the original requests, the number of offers, the selection criteria for selecting an offer, the decisions for selecting an offer, the actual value of the budget being consumed, modifications in the project, spending of the budget and the delivered products/services. Deviations from this can be detected by opening data. Furthermore, the opening of data about the activities and structure of the administrative processes can reveal whether the necessary checks and controls are applied within the process to ensure a proper functioning of the e-procurement system. The patterns that we presented are general patterns that can be used to utilize open data to fight corruption, including the LPSE system. Upon implementation, the pattern needs to be adapted to the context of the situation under study. In further research the patterns can be extended by additional in-depth case analyses. Furthermore, future research can aim at the development of implementation support for opening data to enable the public to scrutinize governmental processes that are prone to corruption.

REFERENCES

[1] S.W. Ambler. 1998. *Process patterns: building large-scale systems using object technology.* Cambridge University Press.

[2] J.C. Bertot, P.T. Jaeger, and J.M. Grimes. 2010. Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies. *Government Information Quarterly2* 27, 3 (2010), 264–271.

[3] W. Ge and S. McVay. 2005. The Disclosure of Material Weaknesses in Internal Control after the Sarbanes-Oxley Act. *Accounting Horizons* 19, 3 (2005), 137–158.

[4] C.W. Gray and D. Kaufmann. 1998. Corruption and development. *Finance and Development* 35, 1 (1998), 7.

[5] M. Hagen and V. Gruhn. 2004. Towards flexible software processes by using process patterns.. In *Proceedings of the Eigth IASTED International Conference on Software Engineering and Applications.* 436–441.

[6] J.A. Hall. 2010. *Information technology auditing.* Cengage Learning.

[7] A.J. Heidenheimer, M. Johnston, and V.T. LeVine. 1970. *Political Corruption* (24 ed.). Holt, Rinehart & Winston, New York. 26–27 pages.

[8] M.F.W.H.A. Janssen and A. Zuiderwijk. 2012. Open data and transformational government. (2012).

[9] LPSE. 2017. LPSE kota Palembang. (2017). http://lpse.palembang.go.id/eproc/

[10] R.B. Marshall and P.J. Steinbart. 2003. *Accounting Information System.* Prentice Hall, New Jersey.

[11] T. Newburn and B. Webb. 1999. Understanding and preventing police corruption: lessons from the literature. (1999).

[12] J.S. Nye. 1967. Corruption and political development: A cost-benefit analysisle. *American Political Science Review* 61, 02 (1967), 417–427.

[13] P. Poerting and W. Vahlenkamp. 1998. Internal strategies against corruption: Guidelines for preventing and combating corruption in police authorities. *Crime, Law and Social Change* 29, 2 (1998), 225–249.

[14] M. Romney, P. Steinbart, J. Mula, and T. Tonkin. 2012. *Accounting Information Systems Australasian Edition.* Pearson Higher Education AU.

[15] J.T. Schickora. 2010. Bringing the four-eyes-principle to the lab. (2010).

[16] D.C. Schmidt, M. Stal, H. Rohnert, and F. Buschmann. 2013. *Pattern-Oriented Software Architecture, Patterns for Concurrent and Networked Objects.* John Wiley & Sons.

[17] J. Silvoso. 1972. *Report of the committee on basic auditing concepts.* Technical Report. 15–74 pages.

[18] L.D. Sousa. 2016. Open government and the use of ICT to reduce corruption risks. (2016).

[19] R.K. Yin. 2003. *Case study research: design and methods.* Sage Publications, Newbury Park, California.