

# Development of a Fraud Risk Control Policy Framework for Public Sector Organizations

Maolana Amin Iskandar  
*Department of Accounting*  
*Faculty of Economics and Business*  
*Universitas Indonesia*  
 Depok, Indonesia  
 oland.maolana@gmail.com

Rafika Yuniasih  
*Department of Accounting*  
*Faculty of Economics and Business*  
*Universitas Indonesia*  
 Depok, Indonesia  
 rafikausman@gmail.com

**Abstract**—This research aimed to develop the framework for a fraud risk control policy, particularly in public sector organizations. This research used qualitative methods to analyze primary data obtained from interviews and secondary data obtained from a literature review. In doing so, this research combines three fraud risk control policy concepts: fraud risk management by KPMG; fraud risk control plan by Badan Pengawasan Keuangan dan Pembangunan Republik Indonesia (BPKP RI / Financial and Development Supervisory Board); and Global Ethics & Integrity Benchmark. The fraud risk control policy currently used by the Ministry of Finance of the Republic of Indonesia is also analyzed. The result of this research is a comprehensive concept of a Fraud Risk Control Policy that is expected to become a reference for public sector organizations to create a more comprehensive fraud control policy, especially on fraud prevention, detection, and response policies.

**Keywords**—*Fraud; Control; Policy; Framework; Public Sector*

## I. INTRODUCTION

As the holder of executive power in the Republic of Indonesia, the Indonesian government is responsible for the good governance of the Republic and to report the nation's annual budget with integrity, accountability, and transparency while at the same time ensuring public participation in the form of taxes and benefits. The Ministry of Finance as one of the state institutions in Indonesia that is required to perform its duties and functions by upholding the principles of integrity, accountability, and transparency. With due regard to the size of the task to be carried out, the Ministry of Finance must perform its functions with good governance. Good governance is necessary because the Ministry of Finance's policies on state revenues (taxes, duties, import duties, and non-tax state revenues) strongly influence public participation to contribute to the state through taxes.

Matei Matei and Drumasu [1] state that from 1980 to 1990 the corporate governance model was adopted and implemented by the public sector in several countries (New Zealand, Australia, and the United Kingdom) as a part of the New Public Management approach. Public sector governance is realized through the delivery of public services that aim to satisfy citizens' needs and provide benefit to the public. In particular, public governance aims at developing and improving management and control mechanisms, taking and fulfilling responsibilities of public personalities (politicians, public servant, etc.) to regain the trust of the citizens.

Aziz, Rahman, Alam, and Said [2] argue that governance in public administration has become a global issue as a result of governance failures, frauds, inefficiencies, corruptions, and other problems in internal control and financial management. Good public governance can be realized by improving accountability. An organization's internal factors, such as integrity system, internal control system, and leadership qualities, are considered to affect accountability improvement in the public sector.

PWC [3], in Mat et al. [4], states that public sector organizations are the most vulnerable to fraud. The public sector becomes particularly susceptible to fraud when not enough time and resources are allocated to assess risks or implement controls to detect, investigate, and mitigate fraud. To prevent fraud, Kusumaningias, Ludigdo, Irianto, and Mulawarman [5] suggest the mechanism of governance because in good governance, regulations are designed in layers to prevent the abuse of roles and procedures.

Kemp [6] explains three main reasons that can trigger rising fraud levels in the public sector: recessionary fall-out, continued cut-backs, and the growth of online services. Adding to that, Ghazali, Rahim, Ali, and Abidin [7] consider that the main cause of fraud in government institutions in Malaysia is poor management practices. To combat fraud in government, there should be more focus on the effectiveness of internal control, action against fraudsters, and oversight by management.

Levi and Burrows [8] explain that fraud can cause many losses or costs to the organization, including fraud loss (transfer cost), anticipatory cost, and the cost of responding to fraud after the event; not to mention the externalities.

Omar [9] states that the adoption of anti-corruption policies is essential for organizations to demonstrate that they already have adequate procedures to prevent theft or fraud. One of the most common anti-corruption policies is the establishment of an anti-corruption agency. While eliminating fraud and corruption is impossible, Mat et al. [4] state the risks of fraud and corruption can be reduced by proper recruitment, training and employment procedures, and adequate internal control.

Danescu, Prozan, and Prozan [10] maintain that internal audit has an important role in the organization to ensure that internal controls, risk management, and governance are well implemented. Internal audit responsibilities are carried out by providing adequate assurance of the adequacy of those

processes. Internal auditing is also responsible for providing recommendations for problem-solving, increased efficiency, and appropriate risk control measures.

Ghazali, Rahim, Ali, and Abidin [7] state that most cases of fraud are found through the work of internal auditors, which demonstrates the importance of internal auditors in protecting government interests from fraud. For fraud prevention policies to be more effective, internal audit units should be given full authority to carry out their duties and their functions must be independent of government management.—(ACFE) survey, reported in the “*Report to The Nations on Occupational Fraud and Abuse: 2016 Global Fraud Study*,” stated that the most fraud cases are to be found in the banking and financial services, government and public administration, and the manufacturing industry. Based on fraud cases involving the government, it is known that cases occurring at the federal or central level have resulted in the highest median loss (\$194,000), which is much higher than at the state (\$100,000) and local (\$80,000) levels. ACFE [11] also explained that the existence of a fraud control policy correlates with lower loss value and faster detection rate. Organizations that have anti-fraud policies experience a lower loss of 14.3–54% than organizations that do not implement the policy. In addition, the existence of an anti-fraud policy makes the organization able to detect fraud faster by 33.3–50% compared with organizations that do not implement the policy.

The Corruption Perception Index (CPI) is one measure used to describe data regarding fraud in Indonesia. Transparency International defines the CPI as an index to measure the perceptions of analysts, employers, and some experts on corruption in the public sector. The CPIs for Indonesia from 2007 to 2016 are presented as Figure 1. Based on Figure 1, it can be seen that the perception of corruption in the public sector is bad and increasing. With a maximum score of 10.00, the CPI score for Indonesia during 2007–2016 is very low (< 4.0); however, the increase in CPI from 2.30 in 2007 to 3.70 in 2015 shows a significant and increasing trend. The Ministry of Finance has a very large responsibility in managing state finances and budgets, so it must implement good governance. To support the implementation of good governance, the Ministry of Finance has established several policies under the “Anti-Corruption Program.” Ministry of Finance [12] explained that the Anti-Corruption Program includes the mapping of sources of corruption, system or performance audit, ministry values, codes of conduct, a whistleblowing system, internal compliance unit, and a reward and punishment mechanism.

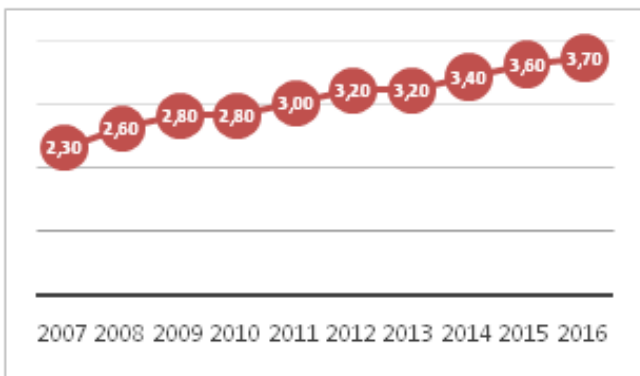


Fig. 1. Graph of Corruption Perception Index Indonesia (2007-2016)  
Source: Transparency International (2007-2017)

In controlling the risk of fraud, the policies established by the Ministry of Finance are not limited to Anti-Corruption Programs. Other policies include anti-corruption socialization, risk management, profiling the track records of officers, reporting and examining officials’ assets, establishment of an Inspectorate for Investigation, investigation procedures, and digital forensic examination. The policy is a combination of mechanisms of fraud risk prevention, detection, and response.

Although several policies have been established to manage fraud risks, they have not fully prevented fraud within the Ministry of Finance. The case of fraud has a negative effect on the organization that will affect the achievement of organizational goals and community perceptions. The case of fraud may occur because the fraud risk control policy currently applied is considered non-comprehensive.

This research aimed to develop a framework for a fraud risk control policy in public sector organizations. A comprehensive framework of fraud risk control policy is expected to become a reference for other public sector organizations in setting policy in accordance with best practices within the organization.

## II. LITERATURE REVIEW

### A. Froud

Murray [13] explains that the word “fraud” derives from the Latin word “*fraus*,” which means deceit. Murray [13] defines fraud as a crime that is not criminal, uses a deceit mode, and is aimed to gain an appreciation or cover up a problem. The Institute of Internal Auditors (IIA) defines fraud as any illegal act characterized by deceit, concealment, or violation of trust. ACFE classifies fraud into three groups:

- *Internal Fraud* or *occupational fraud*, that is, the use of positions within an organization to enrich oneself through intentional abuse. ACFE divides occupational fraud into three groups: corruption, asset misappropriation, and fraudulent statements.
- *External Fraud*, such as a customer providing fake checks when making a payment or a vendor requesting payment from the company for goods/services not provided.
- *Fraud against an Individual*, this type of fraud focuses on individual victims such as identity theft, Ponzi schemes, and phishing

In Dorminey, Fleming, Kranacher, and Riley [14], it is mentioned that Cressey [15] describes the concept of the “fraud triangle” based on the results of research on embezzlement inmates in Illinois. The research concluded that fraud” occurs for three reasons: perceived pressure, perceived opportunity, and rationalization, or together known as the “fraud triangle.”

### B. Fraud Risk Control Policy Framework

Fraud risk requires a specific policy for its handling. Big losses will be borne by the organization if fraud occurs. A comprehensive framework of fraud risk control policy consists of three categories: prevention, detection, and response. The next paragraph will explain the three fraud control policy frameworks along with the attribute details that should be applied by the organization.

### 1) *Fraud Risk Management*

KPMG [16] developed the Fraud Risk Management concept with the aim of developing strategies for the prevention, detection, and response to fraud risks faced by the organization. Fraud Risk Management is manifested by establishing policies, programs, and controls designed to manage fraud risks.

Prevention policies are aimed to reduce the risk of fraud and help prevent the occurrence of fraud risks and comprise *leadership and governance, fraud and misconduct risk assessment, code of conduct, employee and third-party due diligence, and communication and training.*

Detection policies are designed to detect fraud when they occur and are realized through procedures such as *mechanism for seeking advice and reporting misconduct, auditing and monitoring, and forensic data analysis.*

Response policies aim to take appropriate corrective action with regard to fraud losses. The fraud handling policy consists of *investigations, enforcement, and accountability, and corrective action.*

### 2) *Fraud Control Plan*

BPKP RI developed the Fraud Control Plan to formulate controls that can prevent, deter, and facilitate the disclosure of events that indicate corruption. The Fraud Control Plan consists of ten components, each marked by specific attributes. The attribute is a deepening of the organizational governance system that already exists and is influenced by the condition of the organization.

The ten components of the Fraud Control Plan are *standards of behavior and discipline, anti-fraud policy, responsibility structure, fraud risk management, employee concern, customer and community concern, fraud reporting system, investigation procedure, reporting protection, and disclosure to external parties.*

### 3) *Global Ethics and Integrity Benchmark* [17]

In 2009, Joan Elise Dubinsky and Alan Richter created the *Global Ethics and Integrity Benchmarks*. A framework is a tool that can be used by organizations to assess and measure progress in implementing a formal and transparent commitment to ethics and integrity in the workplace. In 2015, Dubinsky and Richter refined the *Global Ethics and Integrity Benchmarks* into 3 clusters:

- **Foundation**, consists of visions and goals, leadership, ethics resource, and legal compliance, policies, and rules.
- **Ethical Culture**, consists of organizational culture, disciplinary and reward measures, corporate social responsibility, ethics communication, and ethics training and education.
- **Ethical Risk Management**, consists of ethics risk assessment, whistleblowing and investigations, conflict of interest, confidentiality and transparency, and bribery and corruption.

### C. *Fraud Risk Control Policy at the Ministry of Finance*

As a public sector organization, the Ministry of Finance faces problems of fraud committed by officials/employees. To

manage the fraud risk, Ministry of Finance has implemented several fraud risk control policies, including:

- **Code of Conduct**, contains obligations and restrictions, as well as sanctions to be obeyed by officials and employees.
- **Risk Management**, consists of activities, communication and consultation, context setting, risk assessment (risk identification, analysis, and evaluation), risk handling, and monitoring and review.
- **Record Tracking of Officials/Officers**, conducted on employees/officers who will receive promotion and mutation.
- **Anti-Corruption Socialization**, regularly conducted to increase understanding, awareness, and concern for officials/employees on the dangers and negative impacts of corruption.
- **Internal Compliance Unit**, embodied in the concept of three lines of defense: management, internal control unit, and Inspectorate General.
- **Inspectorate of Investigation**, was formed in 2004 as an anti-corruption agency to handle several cases of fraud in a comprehensive manner.
- **Reporting and Examination** of the property of officials/employees.
- **Supervision by the internal audit unit**, in the form of audit, topical, thematic supervision, review of financial statements, and monitoring and evaluation of policy implementation.
- **Whistleblowing System**, a grievance channel for the community in reporting fraud cases within the Ministry of Finance. This channel can be accessed through a website, telephone, mail, or directly with a helpdesk officer.
- **Gratification Control Policy.**
- **Investigation Procedures**, guidelines in conducting investigative activities on suspicion of irregularities and misuse of authority.
- **Forensic Digital Examination**, aimed to improve the quality of investigative audits by utilizing information technology.
- **Disciplinary Punishment**, i.e., giving sanctions to officials/employees when they are proven to be in violation

### III. RESEARCH METHODOLOGY

Together with the literature review, this research will integrate some concepts of fraud risk control policies developed by KPMG [16], BPKP [18], and Dubinsky and Richter [19]. Another reference is the fraud risk control policy currently applied by the Ministry of Finance. The integration process is performed by analyzing the characteristics of each component of the fraud risk control policy. Analysis of characteristics is done by considering the impact of the

implementation of the policy on fraud risk control, which is to prevent, detect, or response fraud risk.

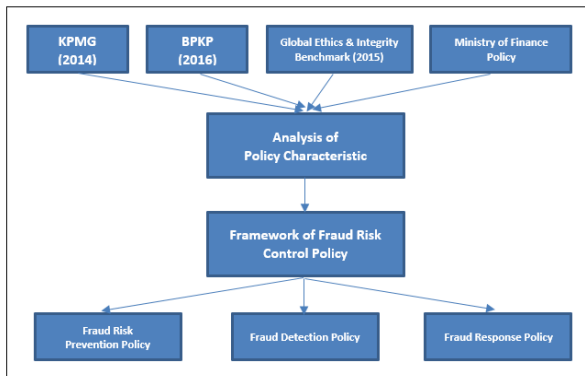


Fig. 2. Chart of Development of the Fraud Risk Control Policy Framework

Based on the results of the analysis, a fraud risk control policy framework will be formulated, consisting of three groups: fraud prevention policy, fraud detection policy, and fraud response policy. An overview of the process of developing a fraud risk control policy framework is described in Figure 2.

#### IV. RESULTS

This section explains the results on the framework of a fraud risk control policy. The policy framework is a combination of KPMG [16], BPKP [18], and Dubinsky and Richter [19], and policies implemented in the Ministry of Finance. Fraud risk control policies are grouped into three categories: prevention, detection, and response. KPMG [16] explains that prevention policies are useful for preventing fraud from the outset, detection policies serve to find fraud as quickly as possible, and response policies are designed to take corrective action and correct the harm caused by fraud.

##### A. Fraud Risk Prevention Policy

###### 1) Leadership

“Leadership” is very important in the successful implementation of a fraud control policy. Leadership is very influential in efforts to control fraud risk through *tone at the top*. Tone at the top will be an example for all officials/employees in doing daily activities. Integrity and ethical leadership can support the establishment of an organizational culture with a high anti-fraud spirit. The role of leadership in encouraging the implementation of fraud risk control policy can be done through:

- a written commitment from the leader of the organization on fraud risk control policy;
- behavior of the organization’s leader in determining tone at the top;
- the oversight structure of the organization’s leader to ensure that internal controls are well underway and fraud risk control policies have been implemented at all levels; and
- assessment of officials’/employees’ perceptions of the integrity and ethics of the organization’s leader.

###### 2) Code of Conduct

The “Code of Conduct” is a formal articulation of organizational culture. The code of conduct is used to shape organizational culture through the inculcation of values of integrity and ethics. Officials and employees in the organization will make the code of conduct as a written guide in performing daily activities. An organizational culture that is formed from the values contained in the code of ethics can be a medium for prevention of fraud. A good code of ethics plays an important role in the prevention of fraud and will include the following elements:

- defined in formal terms of the organization;
- obligations, prohibitions, and sanctions for violations of the code of conduct;
- contains anti-fraud material, whether in prohibition or sanction;
- applies to all organizational components, at all levels; socialized regularly;
- there is a regular evaluation mechanism for compliance with the code; and
- assessment of officials’/employees’ perceptions regarding the material and application of the code of conduct.

###### 3) Anti-Fraud Policy

The embodiment of formal articulation of an anti-fraud policy is in the form of a written commitment from the organization to control fraud risk. The anti-fraud policy becomes the legal basis for the organization in implementing a fraud risk control policy. The inclusion of anti-fraud material in the formal provisions of the organization will be followed by a control mechanism on fraud risks. Based on this, the inclusion of anti-fraud material can be a means of preventing fraud. Implementation of anti-fraud policies in organizations can be realized through:

- the vision and mission of the organization, which includes the anti-fraud policy;
- programs and organizational activities related to fraud risk control;
- budgeting of programs and activities related to fraud risk control;
- performance targets for fraud risk control programs and activities; and
- regulations or policies related to fraud risk control.

###### 4) Internal Audit Unit

The main role of the internal audit unit is to carry out the prevention, detection, and response to fraud within the organization. An independent and competent internal audit unit will enable the organization to benefit greatly in fraud risk control. Strengthening the internal audit function can be done regarding independence, competence, organizational structure, and adequate funding. Some things that must be met for the internal audit unit can perform its role effectively in fraud risk control policy, such as:

- the establishment of internal audit units based on formal policies;
- set duties and functions of the internal audit unit in carrying out its duties, including prevention, detection, and response fraud risks, and evaluation of the effectiveness of internal control policies;
- set performance targets for internal audit units; and
- assessment of stakeholder perceptions related to the performance of the internal audit unit.

#### 5) *Fraud Risk Management*

“Fraud Risk Management” is expected to obtain information about the area with the highest risk of fraud for the organization. Based on the fraud risk assessment results, management can immediately establish a policy to mitigate such risks. The risk mitigation measures will be realized in the form of internal control design in operational procedures. The implementation of Fraud Risk Management within the organization can be realized through the establishment of risk management policies and fraud risk management procedures, including the identification, assessment, and mitigation of fraud risk.

#### 6) *Employee Due Diligence*

The mechanism of “Employee Due Diligence” plays a very important role in fraud prevention. The employee due diligence process can be performed in all positions or positions with very high fraud risks. Employee due diligence is expected to obtain competent candidates of high integrity. Employee due diligence ensures the organization is run by individuals with integrity and free from conflicts of interest. Good employee due diligence mechanisms can be realized as:

- defined in formal terms of organization;
- applies to all mutation and promotion processes, or at least takes into consideration the risks of the positions to be filled;
- materials to be investigated in conducting employee due diligence;
- the obligation to use employee due diligence results in the process of mutation and promotion; and
- assessment of perception of decision-maker of mutation/promotion of an officer/employee to result of employee due diligence and officer/internal staff of organization concerning promotion process and mutation, whether fulfill the criteria of competence, performance, and integrity of related officer.

#### 7) *Third-Party Due Diligence*

A third-party due diligence policy is essential for the organization to avoid losses in the procurement process. The method of selection of bidders should be distinguished by both the complexity and value of the work. The selection of goods/service providers should pay attention to the technical competence and track records of goods/service providers following the auction process. Third-party due diligence is expected to acquire providers of goods/services that are competent and have integrity. A good third-party due diligence mechanism can be realized as:

- defined in formal terms of organization;
- applies to all procurement processes of goods and services;
- materials to be investigated in third-party due diligence; and
- the obligation to use third-party due diligence results in the procurement process of goods/services.

#### 8) *Official and Employee Assets Reporting*

The obligation to report assets to an officer/employee of an organization is necessary to monitor the fairness of property ownership of some high-risk officials. High-risk makes the position vulnerable to corruption and bribery. To avoid conflicts of interest in carrying out their duties, officials should also report other activities outside the main work of the organization. The reporting of business, political, and social activities can be used as material to analyze the potential conflicts of interest. The fraud prevention risk policy will be designed more effectively as it takes into account the equity of ownership of the property as well as the risk of conflict of interest from officials/employees. The assets reporting mechanism can be realized through:

- defined in formal terms of organization;
- applies to all officials/employees;
- components that must be reported, at least including income and expenses, assets and liabilities, payment of personal taxes, business ownership, and activities outside the organization’s duties;
- sanctions for officials/employees not reporting or reporting incorrectly;
- reporting obligations are regularly conducted within a certain period; and
- reporting mechanism that uses information technology for easy reporting and data management.

#### 9) *Communication and Training*

The fraud risk control policy will be more effective when socialized. Socialization should be made to internal and external organizations so that all parties can better understand fraud. In particular, the internal organization also needs to do training related to the implementation of fraud risk control policy and the instilling of integrity and ethics values. Socialization and training can be used as a means to prevent fraud risk through the establishment of a more fraud risk-conscious organizational culture. Socialization and training related to fraud risk control policy can be realized through:

- **Socialization**, stipulated in the formal provisions of the organization, carried out regularly, the socialization participants are internal and external parties, the use of media dissemination widely, performance targets related of socialization, and assessment of perceptions of participants on the effectiveness of the implementation of socialization.
- **Training**, stipulated in the formal provisions of the organization, carried out routinely, the training materials include the application of fraud risk control

policy as well as the inclusion of integrity and ethics values, performance targets of the training, and the assessment of the participants' perceptions on the effectiveness of training.

## B. *Fraud Detection Policy*

### 1) *Whistleblowing System*

A whistleblowing system is a very effective mechanism for detecting fraud. The limitations of the internal audit unit in conducting oversight throughout the organization can be compensated by the provision of a whistleblowing system. Appropriate system planning will affect the management of the whistleblowing system and the success of fraud detection. The whistleblowing system should be supported by data confidentiality and reporting protection mechanisms. These two support mechanisms will require parties, both internal and external, to report fraud cases occurring around them. The elements that must be met for a whistleblowing system to function effectively in doing fraud detection include:

- defined in formal terms of organization;
- data confidentiality and protection of the complainant;
- accessible by internal and external organizations;
- accessible through various media, such as internet, telephone, mail, and others;
- uses information technology;
- complaints management procedures, including procedures for receiving complaints, complaint analysis, and follow-up complaints;
- performance targets for the whistleblowing system; and
- assessment of internal and external party perceptions of the effectiveness of the whistleblowing system.

### 2) *Auditing and Monitoring*

The internal audit unit may stipulate control activities undertaken by the unit as a means of detecting fraud. Control activities are undertaken by internal audit units in the form of audit and monitoring. Audit and monitoring results conducted by the internal audit unit include the implementation of operational activities that are not in accordance with the provisions. The findings of audit and monitoring, especially those considered significant, may be an indication of fraud. Therefore, auditors conducting audit and monitoring must improve their competence to detect fraud indications through findings of non-compliance with procedures or conditions. For the audit and monitoring activities to be effective, several conditions must be met:

- authority of the internal audit unit to audit and monitor;
- audit and monitoring procedures;
- risk-based audit;
- follow-up on audit and monitoring results;
- assessment of audit and monitoring;
- performance targets for audit and monitoring;

- budgeting for audit and monitoring; and
- auditors who have adequate competence and capability to audit.

### 3) *Examination of Officials'/Employees' Assets Reporting*

Examination on assets reporting can be an effective method to detecting fraud. Examination is done by examining the truth and fairness of reporting for property owned by officials/employees. The findings of the results of the examination that indicate mismatches and misalignment of the reported asset may be an indication of fraud committed by the officer/employee. For unreported and unfair assets, this can be followed-up by checking the source of the acquisition of the property. From the results of further examination is expected to obtain information about the case of fraud, which became the source of acquisition of the property. In order for the examination activities to run effectively, the following conditions must be met:

- authority of the internal audit unit to perform the examination;
- examination procedure;
- sanctions for officials/employees on the findings of the examination;
- assessment of examination;
- performance targets for examination;
- budgeting for examination; and
- auditors who have adequate competence and capability.

### 4) *Gratification Control Policy*

Gratification is one of the most common forms of fraud in an organization. The organization should set policies to regulate gratuities to officials/employees. The policy is used to regulate the handling mechanisms for gratuities that have been received by officials/employees to be subsequently reported to the relevant units. Reporting on gratuities received by officials/officers can be a mechanism to detect fraud cases in the workplace of the official/employee. Therefore, it is necessary to prepare a structured and effective gratification reporting handling mechanism so that the gratification reporting information can be followed up by efforts to detect fraud cases. The gratification control policy will be effective if it fulfills the following:

- defined in formal terms of organization;
- gratification reporting mechanism to related units;
- minimum information to be reported by gratuity recipients;
- applies to all officials/employees within the organization;
- sanctions for officials/employees not reporting or reporting incorrectly on the gratification received;
- mechanism for handling or follow-up on gratification reports; and

- performance targets for gratification control.

### 5) *Analysis of Digital Data and Information*

Organizational activity will produce digital data with a large quantity of both financial and non-financial data. In addition, information related to the organization through the internet can also provoke the reactions and perceptions of its readers. Organizations can analyze both types of data as a method to identify fraud. Fraud indication can be found through a deep process of analysis so that anomaly in the dataset can be obtained.

Analysis of digital data and information can support the policy of fraud risk control comprehensively. The data and information analyzed most include at least two elements: organization transaction data and information related to the organization that is on the internet. The results of data analysis and digital information can be used as a mechanism for fraud detection. The results of digital data and information analysis can also be used as an ingredient for the preparation of a fraud prevention risk policy. Digital data and information analysis activities will be effective if they meet the following:

- defined in formal terms of organization;
- authority to access organizational transaction data in real-time;
- authority to access information related to existing organizations on the internet;
- procedure of analysis of digital data and information;
- completeness of equipment and software to perform analysis of digital data and information;
- follow-up procedures for the results of analysis of digital data and information;
- utilization of results of analysis of digital data and information for fraud risk control policy;
- performance targets for analysis of digital data and information;
- budgeting for analysis of digital data and information; and
- employees who have adequate competence and capability to perform analysis.

## C. *Fraud Response Policy*

### 1) *Investigations*

The investigation is the first activity performed by the organization when a fraud case has occurred. The investigation is conducted to gather evidence and facts, so that information about an act of fraud becomes clear. The organization shall establish guidelines for the investigation to be conducted systematically and professionally. The results of the investigation are expected to assist the organization in making decisions to follow up the fraud case that occurred. An effective investigation process will take place when the following points are met:

- defined in formal terms of organization;
- authority in conducting investigations, at least including data and information requests;

- confidentiality of all data in the investigation process;
- procedures for planning, implementing, and reporting investigations;
- monitoring of follow-up on the recommendation of investigation result;
- assessment of the investigation;
- performance targets for investigation;
- budgeting for investigation; and
- auditors who have adequate competence and capability to conduct investigations

### 2) *Collection of Audit Evidence on Digital Data*

One of the challenges faced in the process of handling fraud is the use of information technology by the perpetrators. To deal with this, the auditor needs to have the ability to collect audit evidence on digital data. Digital data is the output of an information system. Digital data that has the potential to become audit evidence is not limited to transaction data; that is, the output of the organization's information system also includes digital data from the fraud perpetrators' communications devices. To confront this condition, the organization shall establish a policy related to the collection of audit evidence of digital data. The following elements must be met for the policy of collecting audit evidence on digital data in order for it to be effectively implemented:

- defined in formal terms of organization;
- authority of access to organizational transactions, systems, and data;
- authority of access to personal communication devices, systems, and data of internal officials/employees;
- confidentiality of personal communication data of internal officials/employees;
- procedure of collecting audit evidence on digital data;
- guidelines for documentation and reporting;
- completeness of tools and software;
- performance targets of audit evidence collection activities on digital data;
- budgeting of audit evidence collection activities on digital data; and
- personnel who have sufficient competence and capability to collect audit evidence on digital data.

### 3) *Standard of Discipline*

After the case of fraud is revealed with evidence obtained from the investigation, the organization must then mete out punishment to the fraud perpetrator(s). The application of disciplinary punishment to perpetrators of fraud should be done consistently. This will send a strong signal to other fraud offenders that the organization is serious about enforcing the rules. Fraud perpetrators are expected to receive a deterrent effect after receiving disciplinary punishment. The internal organization is expected also to become more aware and alert

about the consequences that must be borne when fraud occurs. Based on this, the application of disciplinary sanctions functions in two ways: prevention and response to fraud. Good disciplinary sanctions play an effective role in the fraud and can be realized through the following points:

- defined in formal terms of organization;
- types of violations and disciplinary sanctions;
- procedures for determining the types of sanctions and imposing sanctions on the perpetrators of fraud;
- applies to all organizational components, at all levels;
- performance targets; and
- assessment of internal parties' perceptions regarding the implementation of disciplinary sanctions for fraud perpetrators.

#### 4) *Corrective Action*

Fraud will always cause harm to the organization, both in material and non-material forms. The organization must take some action to fix the losses incurred due to fraud. Corrective actions that can be taken by the organization include restoring material losses, improving ineffective control procedures, and communicating the results of the organization's actions in handling fraud cases to all interested parties. Improvement actions undertaken by the organization are expected to restore the losses that arise and improve the image of the organization damaged by the fraud case. Policies related to corrective action will be effective in the efforts of fraud can be realized through the following points:

- defined in formal terms of organization;
- material or financial compensation procedures;
- procedures for improvement of internal control over operational activities of the organization;
- communication procedure of fraud case handling; and
- assessment of internal and external party perceptions related to organizational actions in making improvements to fraud cases.

#### 5) *Confidentiality*

Organizational activities produce important information, both internal and external. Information collected during the fraud case investigation process is also confidential information for the organization. Such information requires special handling so as not to spread freely to unauthorized parties. The distribution of important information belonging to the organization to unauthorized parties can be categorized as a fraud. To avoid this, organizations need to make policies to regulate data confidentiality. Effective policies to manage data confidentiality must meet the following:

- defined in formal terms of organization;
- classification of confidential data and documents;
- sharing of access to confidential data and documents;
- confidentiality of all data and documents related to investigative activities;

- sanctions for parties who disseminate confidential data and documents;
- internal socialization related to data confidentiality policy; and
- assessment of internal and external party's perception of the implementation of data confidentiality policy.

#### 6) *Informant Protection*

Whistleblowing is known as one of the most effective means of fraud detection. A good whistleblowing system should be accompanied by provisions to protect those who report fraud. The protection granted to the complainant is aimed to avoid any negative action or policy directed against the complainant. Effective informant protection policies are expected to increase the participation of all parties to report fraud through the whistleblowing system. Effective informant protection policies can be realized through the following:

- defined in formal terms of organization;
- informant protection procedures;
- cooperation with authorized apparatuses, such as witness protection agencies; and
- socialization of the informant protection policy to internal and external parties.

#### 7) *Disclosure to External Parties*

The case of fraud faced by the organization has varying degrees of difficulty to uncover it. Fraud response policies that have been implemented by organizations are not always able to uncover the case of the fraud. When faced with a large fraud case and requires more detailed handling beyond the organization's capabilities, another step is needed to address it. Faced with these conditions then the steps that can be taken by the organization is to reveal the case to external parties. External parties are expected to assist the handling of these fraud cases. By disclosing to external parties is expected process handling fraud case becomes more effective. To realize the disclosure policy to an effective external party, it must meet the following:

- Defined in formal terms of organization;
- Classification of fraud cases that can be disclosed to external parties;
- Fraud case disclosure procedures to external parties;
- External parties eligible to receive fraud case disclosure;
- Cooperation with external parties to handle fraud cases.

#### D. *Analysis*

In the process of formulating a fraud risk control policy, public sector organizations should pay attention to several issues for the resulting policy to be of quality and to function effectively. For the fraud risk control policy to be qualified it must include the following:

- defined in the form of formal organization policy;
- planning, implementation and reporting procedures;



- monitoring of policy implementation;
- applicable to all organizational components, at all levels;
- performance targets for policy implementation; and
- planning and budgeting activities.

There are additional elements necessary for a fraud risk control policy to be qualified and to function effectively. Some of the specifics adjust to the characteristics of each policy.

In addition, analysis of the implementation of a fraud risk control policy will use the self-efficacy theory of Bandura [20] in Feist and Feist [21]. Based on self-efficacy theory, the fraud risk control policy framework is aimed at reducing the chances of fraud in the organization. The fraud prevention risk policy is intended to convince related parties that committing fraud will be difficult; that is, fraudulent behavior becomes difficult when the organization has implemented policies to prevent its occurrence.

The fraud detection policy aims to convince relevant parties that all fraud acts will be known immediately through several mechanisms. Fraud perpetrators find it difficult to hide their actions because the organization has implemented a continuous policy to detect fraud. The fraud detection mechanism also provides channel choices for all parties to get involved in uncovering fraud.

The fraud response policy aims to send the message that all fraud cases will be handled professionally, carefully, and with integrity. The fraud response policy also carries the message that all fraud actors will be subject to severe punishment, a deterrent effect; in other words, fraud is not worth the financial gain. The implementation of a fraud risk control policy that is consistently and continuously applied is expected to form an anti-fraud organizational culture.

## V. CONCLUSION

The framework for a fraud risk control policy, which is the reference in this research, is fraud risk management by KPMG and the fraud control plans of BPKP and the Global Ethics and Integrity Benchmark by Dubinsky and Richter. Another reference in this research is the fraud risk control policy applied by Ministry of Finance. Based on these four references, an analysis has been conducted to develop a comprehensive fraud risk control policy framework that can be applied to public sector organizations. The framework for the fraud control policy generated by this research is divided into three groups: fraud prevention policy, fraud detection policy, and fraud handling policy. The following describes the details of the fraud risk control policy framework:

- Fraud Risk Control Policy, consists of leadership, code of conduct, anti-fraud policy, internal audit unit, fraud risk management, employee due diligence, third-party due diligence, official and employee assets reporting, and communication and training.
- Fraud Detection Policy, consists of whistleblowing system, auditing and monitoring, examination of official & employee assets reporting, gratification control policy, analysis of digital data and information.

- Fraud Response Policy, consists of investigations, a *collection of audit evidence on digital data*, the standard of discipline, corrective action, confidentiality, informant protection, and disclosure to external parties.

The fraud risk control policy framework is aimed at reducing the chances of fraud occurring within the organization. The fraud prevention risk policy is intended to convince related parties that fraud will be difficult. The fraud detection policy aims to convince related parties that all fraud acts will be known immediately through several mechanisms. The fraud response policy aims to send the message that all fraud cases will be handled professionally, carefully, and with integrity. The fraud response policy also carries the message that all fraud actors will be subject to severe punishment, a deterrent effect; thus, fraud is not worth the financial gain. The implementation of a fraud risk control policy and its consistent application are expected to form an organizational culture with integrity and an anti-fraud mindset.

## REFERENCES

- [1] M. Ani and D. Ciprian, Corporate Governance and Public Sector Entities. Paper presented at 4th World Conference on Business, Economics and Management, 2015
- [2] M. A. A. Aziz, A. H. Rahman, A. Hilmi, M. M. Alam, and J. Said, "Enhancement of the Accountability of Public Sectors through Integrity System, Internal Control System and Leadership Practices: A Review Study," Paper presented at 7<sup>th</sup> International Conference on Financial Criminology 2015, Oxford, United Kingdom, 2015
- [3] PWC, Fighting fraud in the public sector, The government and public sector extract from PwC's Global Economic Crime Survey, Australia, 2011.
- [4] T. Z. T. Mat, S. N. F. S. M. Nazri, F. M. Fahmi, A. M. Ismail and M. Smith, "Assessing The Fraud Prevention Mechanisms in Malaysian Government Agencies," Malays. Accounting. Rev, Vol. 12(2), pp. 141-169, 2013.
- [5] R. Kusumaningtias, U. Ludigdo, G. Irianto and A. D. Mulawarman, "Rethinking of Corporate Governance," Paper presented at 3<sup>rd</sup> Global Conference on Business and Social Science-2015, Kuala Lumpur, Malaysia, Science Direct database, 2015.
- [6] G. Kemp, "Fighting public sector fraud in the 21st century," Computer Fraud & Security, 16-18. November, ScienceDirect database, 2010.
- [7] M. Z. Ghazali, M. S. Rahim, A. Ali and S. Abidin, A preliminary study on fraud prevention and detection at the state and local government entities in Malaysia. Paper presented at International Conference on Accounting Studies 2014, Kuala Lumpur, Malaysia, 2014.
- [8] M. Levi, and J. Burrows, "Measuring The Impact of Fraud in the UK: A Conceptual and Empirical Journey," Br. J. Criminology, Vol. 48(3), pp. 293-318, 2008. <http://www.jstor.org/stable/23639088>
- [9] N. Omar, "Corporate Integrity as an Antidote to Corruption and Sustenance of Organizational Development: The Renewed Role of Management Accountants," Malays. Accounting. Rev, Vol. 14(2), pp. 109-136, 2015.
- [10] T. Danescu, M. Prozan and R. D. Prozan, "Perspective regarding accounting-corporate governance-internal control," Procedia Econ. Financ, vol. 32, pp. 588-594, 2015.
- [11] ACFE, "Report to The Nations on Occupational Fraud and Abuse: 2016 Global Fraud Study," Association of Certified Fraud Examiners, Inc., 2016.
- [12] Ministry of Finance (MoF), Government of Indonesia (n.d.) 'Indonesia National Budget 2017. Accessed 18 May 2017 < <https://www.kemenkeu.go.id/>>
- [13] J. G. E. Murray, "Some aspects of fraud, control and investigation," J. Criminal Law, Criminology, Police Sci, vol. 49(1), pp. 78-88. 1958.
- [14] J. Dorminey, A. S. Fleming, M. Jo-Kranacher, J. Riley and A. Richard, "The Evolution of Fraud Theory," Issues Accounting Edu, vol. 27(2), pp. 555-579, 2012.

- [15] D. R. Cressey, "The criminal violation of financial trust," *Am. Sociological Rev*, vol. 15 pp. 738–743, 1950. <http://dx.doi.org/10.2307/2086606>
- [16] KPMG Forensic, *Fraud Risk Management: Developing A Strategy for Prevention, Detection, and Response*. China: Author, 2014.
- [17] J. E. Dubinsky and A. Richter, *Ethics and In-tegrity Best Practices Tool: Global Ethics and Integrity Benchmarks*. QED Consulting, New York: United States, 2009.
- [18] Badan Pengawasan Keuangan dan Pembangunan. (November 2016). *Modul Fraud Control Plan*.
- [19] J. E. Dubinsky and A. Richter, *Global Ethics and Integrity Benchmarks*, Maryland & New York: USA, 2015.
- [20] A. Bandura, "Social cognitive theory: an agentic perspective," *Annu. Rev. Psychol*, vol. 52, pp. 1–26, 2001. 10.1146/annurev.psych.52.1.1 [PubMed] [CrossRef].
- [21] J. Feist and G. J. Feist, *Theories of Personality Seventh Edition*. McGraw-Hill Primis, 2009.