Asia Pacific Fraud Journal
E-ISSN: 2502-695X, ISSN: 2502-8731
Volume 4, Nomor 1 (January-June) 2019
http://apfjournal.or.id/index.php/apf

INHERENT FRAUD RISK ASSESSMENT: ANALYSIS OF MAIN TASKS TO MINIMIZE FRAUD RISK
(Case Study of an Industrial Supervisory in Indonesia)

Yulia Nurlita and ✉Edward Tanujaya
Faculty of Economics and Business, Universitas Indonesia

ARTICLE INFORMATION

Article History:
Received Nov 16, 2018
Revised Dec 14, 2018
Accepted Dec 1, 2018

JEL Classifications:
D73; G32; D12

DOI:
10.21532/apfj.001.19.04.01.01

ABTRACT

This research aims to analyze and provide views on inherent fraud risk of an Industrial Supervisory in Indonesia. The inherent fraud risk analysis will be examined using fraud risk assessment methods presented in COSO: 2016. Based on observations of the main tasks and work units of the organization, there are 18 fraud schemes identified. The results of this study indicate that the four highest fraud schemes are "Extortion to the 3rd party", "Conflict of interest in licensing", "Conflict of interests in external arrangements", and "Conflict of interest in Enforcement/inspection". As for related tasks, there are three things that must be considered: management of information systems, logistics, and industrial supervision.

Keyword: work unit, main task, fraud scheme, level of inherent fraud risk

1. INTRODUCTION

COSO: 2016, states that the risk of fraud in each organization is impossible to be eliminated. However, by implementing the principles identified by COSO: 2016, it can be believed that every organization is able to improve the prevention of fraud or in other words, minimize fraud. Fraud risk assessment is carried out based on existing inherent fraud risk. Inherent fraud risk is a risk of fraud where the condition of the organization is assessed without considering the existing control system. The inherent fraud risk is the first step taken so that all fraud risks can be identified.

There are three important focus that can be used as an approach in assessing optimal inherent risk, which is focused on important issues in the organizational structure; re examine the significance of the results of inherent risk; and understand the processes contained in inherent risk that have been identified (Shailer, Wade, Willett, & Yap: 1998). Every organization has an inherent fraud risk in accordance with the structure and function of the organization itself. Some organizations that have similar functions usually have almost the same inherent fraud risk. The inaccuracy of organizations in identifying inherent fraud risk can lead to errors in preventive actions and audit activities (Beasley, Carcello, & Hermanson: 2001). Appropriate identification of inherent fraud risk in an organization can provide input to the organization regarding the appropriate form of prevention in handling fraud cases. Inherent fraud risk can be categorized into several categories that are in accordance with the needs of the organization.

The problems examined in this study are what factors influence inherent fraud risk in an industrial supervisory; what is the level of occurrence, significance, and

✉ Corresponding author :
Address : -
Email : edward_tanujaya@yahoo.com

the level of inherent fraud risk that exists in an industrial supervisory; what are the efforts to minimize fraud risk in an industrial supervisory?

This study focuses on knowing what factors cause to inherent fraud risk in one organization through analysis of the main tasks, knowing the level of occurrence, the level of significance, and the spread of inherent fraud risk levels in one organization through analysis of organizational structure and authority, and also providing an alternative effort that can be done to minimize fraud risk in one organization based on best practices and other standards of fraud risk assessment.

2. THEORICAL BASIS

Fraud

COSO : 2016, states that fraud is an act or negligence that is intentionally designed to deceive other people and cause victims to suffer and / or the perpetrators achieve profits. The term Fraud generally includes activities such as theft, corruption, embezzlement, conspiracy, extortion, money laundering, and bribery. The definition of fraud adopted by each country can vary depending on the regulations set by each country (CIMA: 2009).

According to ACFE: 2008, there are 3 main categories of fraud that are influential in an organization: asset misappropriations, fraudulent statements, and corruption. Along with the development of fraud cases, according to the ACFE: 2018a, falsification of reports has led to one type of report, namely financial statements.

Several factors that can provide opportunities for fraud in an organization are the duties and functions of the organization, the environment of the organization's existence, the effectiveness of internal control, the culture of organizational integrity (ACFE: 2016).

Risk Management

Every organization that comes from various types and sizes will face the uncertainty, both from internal and external sides, which can interfere in achieving its objectives. To convince organizations to be able to deal with these disturbances, a risk management strategy that is repeatedly and continuously applied is needed (ISO 31000: 2018).

ISO 31000: 2018, explains that risk management is one technique that can guard an organization in achieving its objectives. Risk Management is implemented and embedded in the determination of organizational strategy and decision making. Risk management is part of corporate governance and leadership as a basis for reference in managing all levels in an organization. The contribution of risk management in an organization is in the form of input related to the improvement of the organization's management system. In risk management, all forms of interaction with stakeholders are considered and assessed, this assessment is called the internal and external context of the organization.

Generally, the implementation of risk management is carried out in three categories: the application of risk management principles, the design and implementation of a risk management framework, and the implementation of the risk management process. The principles of risk management in ISO 31000: 2018, are integrated; structured and comprehensive; customized; inclusive; dynamic; based on the best information available; human and cultural factors; and continual improvement.

A risk management framework is created to help organizations integrate risk management into their activities. The effectiveness of risk management highly depend on the successful integration of risk management with the decision making process and organizational governance. According to ISO 31000: 2018, the risk management framework consists of leadership and commitment, integration, design, implementation, evaluation, and improvement.

The risk management process is a form of systematic implementation of

risk management policies, procedures and practices. Organizational behavior and culture must be considered as a dynamic variable during the process of implementing risk management. The risk management process according to ISO 31000: 2018 consists of communication and consultation; determination of scope; context and criteria; risk assessment; risk treatment; monitoring and review; and also recording and reporting.

Fraud Risk Management

In line with ISO 31000: 2018, COSO: 2013 has outlined the standards of the components of the framework as well as internal control principles which generally consist of 5 components and 17 principles:

1) Control Environment
   1. Demonstrates commitment to integrity and ethical values
   2. Exercises oversight responsibility
   3. Establishes structure, authority, and responsibility
   4. Demonstrates commitment to competence
   5. Enforces accountability
2) Risk Assessment
   6. Specifies suitable objectives
   7. Identifies and analyzes risk
   8. Assesses fraud risk
   9. Identifies and analyzes significant change
3) Control Activities
   10. Selects and develops control activities
   11. Selects and develops general controls over technology
   12. Deploys through policies and procedures
4) Information & Communication
   13. Uses relevant information
   14. Communicates internally
   15. Communicates externally.
5) Monitoring
   16. Conducts ongoing and/or separate evaluations
   17. Evaluates and communicates deficiencies

COSO: 2016 regulates guidelines in fraud risk management. The principles adopted in fraud risk management are related to COSO: 2013, while the principles in fraud risk management are as follows:

1) The organization establishes and communicates a fraud risk management program that demonstrates the expectations of the board of directors and senior management and their commitment to high integrity and ethical values regarding managing fraud risk. In COSO: 2013 this principle is related to the Environmental Control component.
2) The organization performs compherensive comprehensive fraud risk assessment to identify specific fraud schemes and risks, assess their likelihood and significance, evaluate existing fraud controls activities, and implement actions to mitigate residual fraud risks. In COSO: 2013 this principle is related to the Risk Assessment component.
3) The organizations selects, develops, and deploys preventive and detective fraud control activities to mitigate the risk of fraud events occuring or not being detected in a timely manner. In COSO: 2013 this principle is related to the Control Activity component.
4) The organization establishes a communication process to obtain information about the potential fraud and deploy a coordinated approach to investigation and corrective acPtion to address fraud appropriately and in a timely manner. In COSO: 2013 this principle is related to the Information and Communication component.
5) The organization selects, develops, and performs ongoing evaluations to ascertain wheter each of the five principles of fraud risk management is present and functioning and communicates Fraud Risk Management Program deficiencies in a timely manner ti parties responsible for taking corrective action, including senior management and the board of directors. In COSO: 2013 this principle is related to the Monitoring component.

Fraud Risk Assessment

Fraud risk assessment in detail is described

in COSO: 2016. A comprehensive approach needs to be applied in fraud risk assessments within the organization. In implementing the fraud risk assessment, there are 12 main focuses that must be considered as follows:

1) The manager must contribute as part of the team in the fraud risk assessment.
2) Fraud risk assessment is conducted at all levels in the organizational structure.
3) Fraud risk assessment needs to identify the internal and external context of the organization.
4) Fraud risk assessment must identify all potential fraud in the organization
5) Fraud risk assessment must specifically identify the override controls of each manager.
6) Fraud risk assessment estimates the possibility of risk occurrence and the magnitude of the risk impacts that will be caused.
7) Fraud risk assessment must assess the overall behavior of employees that have the potential to meet all aspects of triangle fraud.
8) Fraud risk assessment identifies the level of fraud control that has been applied in an organization.
9) Fraud risk assessment determines the appropriate response in dealing with fraud risk.
10) Fraud risk assessment is conducted based on the right data and techniques in assessing and determining the appropriate risk fraud response.
11) Fraud risk assessment is conducted periodically and sees changes that occur in fraud risk.
12) Fraud risk assessment must be documented.

The steps for implementing the fraud risk assessment are as follows: determine the team in implementing the fraud risk assessment; identify all fraud schemes and fraud risks; estimate the level of occurrence and significance of the fraud risk scheme; determine all employees and organizational structures that have high potential for fraud triangle; identify the level of internal control and effectiveness; make appropriate assessments and responses to residual risk; determine the risks that need to be mitigated; document the results of risk assessments; do periodically, take the fraud risk assessment step again to assess changes.

Stakeholders Analisis

According to Eden & Ackermann: 1998, by identifying the level of influence (power) of stakeholders in an organization and the level of interest of stakeholders in an organization, the organization can group stakeholders according to the appropriate treatment for each group of stakeholders. Eden & Ackermann: 1998 simplifies the way in analyzing stakeholders in the form of a matrix as follows:

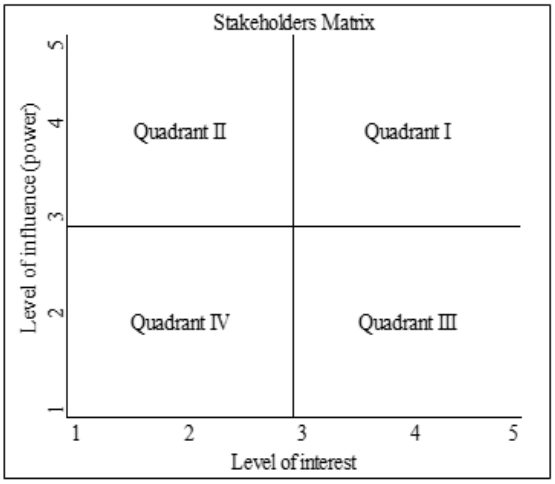

Figure 1
Stakeholders matrix

Stakeholders in quadrant I are Key players. With a high level of interest and a high level of power towards the organization, the organization needs to meet expectations and always report developments to stakeholders in this quadrant. The right treatment for stakeholders in quadrant I is "manage closely".

Stakeholders in quadrant II are stakeholders who have a high level of power towards the organization, but the level of interest is low. The thing that needs to be fulfilled by the organization towards stakeholders in quadrant II is to always fulfill all expectations. Thus, the

right treatment for these stakeholders is "keep satisfied".

Stakeholders in quadrant III are stakeholders who have a high level of interest, but the power level of stakeholders in the organization is low. The needs of stakeholders in this quadrant are organizational informations and developments. The right treatment for these stakeholders is "keep informed".

Stakeholders in quadrant IV are stakeholders who are categorized as stakeholders who have the lowest priority. Stakeholders have a low level of power and interest for the organization. Organizations only need to monitor all forms and actions of stakeholders in this category.

Dimension of National Culture

According to Hofstede: 1983, culture is part of the conditions we feel together in one nation, region, or group. Culture influences the ability of the community to manage the organization well. In his writing, Hofstede divides into 4 cultural dimensions:

1) Large or small power distance (Dimension 1)
   This dimension measures how people perceive and accept power differences. In cultures with great power distance, individuals tend to accept autocratic or paternalistic power relations. However, in cultures that have little power distance, individuals will accept more democratic power relations.
2) Individualism vs. collectivism (Dimension 2)
   In individualist culture, individuals tend to develop and display their personalities and choose their own affiliations. In the culture of collectivism, individuals are defined as members of a group on a long-term basis.
3) Masculinity vs. Femininity (dimension 3)
   This cultural dimension is closely related to the different attributes of traditional gender regulations. Masculine culture is expected to have higher competitiveness, firmness and accumulation of wealth. While feminine culture is expected to have an attitude in respecting relationships and a better quality of life.
4) Avoidance of uncertainty: weak vs. strong (Dimension 4)
   This dimension measures the attitude of a community in dealing with risk. In cultures with a strong level of avoidance of uncertainty, individuals tend to prefer explicit rules and structured formal activities. Conversely, in cultures with a degree of avoidance of weak uncertainty, individuals prefer flexible rules and informal activities.

In subsequent studies, Hofstede & Bond: 1988 developed the 5th cultural dimension:

5) Long term orientation (Dimension 5)
   This dimension measures the value associated with the future. The opposite of this dimension is short-term orientation, which is described as a society that prioritizes tradition, fulfills social expectations, and maintains the current state (status-quo).

In his research, Hofstede: 1993 compared scores in ten countries related to these 5 dimensions (America, Germany, Japan, France, Netherlands, Hong Kong, Indonesia, West Africa, Russia and China), with the following results (Tabel 1).

3. METHOD

Sample Selection

The organization that will be discussed in this case study is one of the organizations engaged in industrial supervision. The government-owned organization formed by this Law has a vision of being a trusted supervisory institution, protecting the interests of consumers and society, and being able to realize the industry as a pillar of national economy that is globally competitive and can promote public welfare. The organization's mission is to realize the implementation of all activities in the industry on a regular, fair, transparent and accountable basis; realize a financial system that grows sustainably and stably; protect the interests of consumers and society.

Table 1
Comparison of Cultural Dimensions in 10 Countries

Country	Dimension 1	Dimension 2	Dimension 3	Dimension 4	Dimension 5
America	40	91	62	46	29
Germany	35	67	66	65	31
Japan	54	46	95	92	80
Franch	68	71	43	86	30
Netherland	38	80	14	53	44
Hong Kong	68	25	57	29	96
Indonesia	98	14	46	48	25
West Africa	77	20	46	54	16
Russia	95	50	40	90	10
China	80	20	50	60	118
Average	65,3	48,4	51,9	62,3	47,9

Source: Data Process

This organization is led by a collective collegial group, which in this study is called the Supreme Leader. By adhering to a one-tier system, where the Commissioners also act as executors of operational activities, this organization is equipped with 3,880 employees and spread across 35 cities in Indonesia. The level of bureaucratic positions in this organization consists of 9 levels besides the highest leadership.

The tasks, functions, and authority carried out by this organization are divided into 2 parts, namely tasks and functions related to the technical field of the organization, and the tasks and functions that are supporting in running the organization. The work units that carry out the tasks and functions included in the technical field of the organization are as follows:

1) Industrial Regulations and Supervision
   Industrial regulation and supervision are divided into 3 major groups, namely sector 1, sector 2, and sector 3. In this regulation and supervision unit, employees carry out periodic monitoring tasks on: industry reports, industrial contribution amounts, and keep the industry compliance with the regulation. The industrial licensing and drafting of the industrial regulation concept were also carried out by the supervisors. In addition, this section also provides data and other statistical information related to each industry.
2) Integrated Regulation and Supervision
   Integrated regulation and supervision focuses more on industrial supervision that runs business units in all major sectors as described in number 1. Employees who carry out activities in this unit only carry out periodic monitoring of industrial activities in an integrated manner and carry out supervision in terms of crisis early warning system.
3) Industrial Investigation
   Some industries that violate the regulation will be investigated by investigators who are under this unit. The report on industrial violations was carried out by the Industrial Regulation and Supervision unit and then carried out an investigation by the Industrial Investigation unit
4) Consumer Education and Protection
   In consumer education and protection, employees monitor and work together with the industry to increase the level of public understanding of the industry. In addition, this unit can also be a mediator in the event that disputes between industry and industrial consumers cannot be handled further in their respective industries.

The tasks and functions of this organization which are supporting functions consist of seven work units. Some of these units, most of them, only carry out the task of developing policy tools and compilation, while daily planners, implementers, and supervisors were distributed to each work unit. The seven units are:

1) Organization and Human Resources (HR) Management
   The organization and HR management unit establishes the organizational structure and recruitment, placement, and payroll of HR. The implementation of activities related to the fulfillment of effective formations prioritized from the recomendation of each work unit. HR management, such as attendance monitoring activities, HR facilities, recommendations for imposing sanctions, Individual Performance Indicators assessment, are monitored and implemented in each work unit.
2) Strategic and Logistics Management
   Strategic management functions as a unit that implements and monitors balanced scorecards in the organization. This unit formulates the direction of the organization's strategy map and then formulates its performance indicators. These performance indicators are submitted from each work unit which in the implementation are assisted by KPI's managers in each work unit. The KPI's manager also regularly monitor the achievement of performance indicators and report to strategic management. Logistics units carry out procurement of office supplies such as office buildings, work spaces, office stationery, and so on. In carrying out its duties, the logistics unit is assisted by the sixth level manager that has specialists in identifying non-information technology assets and office equipment needs.
3) Management of Information Systems
   In supporting its activities, organizations form an information system management unit as a unit that will create information systems needed. Every work unit submit the user requirements of the information system requirements to support their duties, and the information system management unit that will develop the system or conduct a development system auction. In addition to the procurement of information systems, this unit is also tasked with the procurement of equipment and information technology assets. This procurement is based on the identification of the needs of information technology equipment and assets identified by each work unit.
4) Financial Management
   Financial management is a management that is spread in each work unit. The central unit of Financial management publishes the financial statements of the organization, however, budget planning, budget execution, and budget accountability are delegates to each work unit.

Heatmap of Risk Level			Level of Impacts				
			1	2	3	4	5
			Very Low	Low	Medium	High	Very High
Level of likelihood	5	Very High	Medium	High	High	Very High	Very High
	4	High	Low	Medium	High	Very High	Very High
	3	Medium	Low	Low	Medium	High	Very High
	2	Low	Very Low	Low	Medium	High	Very High
	1	Very Low	Very Low	Low	Low	Medium	Very High

Figure 2
Heat Map Penilaian Risiko

5) Legal Unit
The Legal Unit has the task of harmonizing regulations. Each work unit identifies and designs its own regulatory needs to support its work. Regulatory design is made up to a clean draft that is ready to be issued as a regulations. This clean draft will be take some legal review by the legal unit before it is signed. In addition to legal review, the legal unit also assists employees who carry out their duties in the organization in connection with judicial cases (both as witnesses and defendants)

6) Training Agency
The Training Agency organizes employee development programs in the form of in-house training, domestic non-in-house training, foreign non-in-house training, scholarships, employee assessments, and industrial training activities as a form of industrial contribution return programs. In carrying out its duties, the education and training body is assisted by learning partners spread across all work units. Learning partners carry out learning need analysis in each work unit, and then sent to the training agency to be adjusted to the availability of the budget. Effective monitoring is also carried out by learning partners and Training Agency together.

7) Internal Audit and Risk Management
Internal Audit reassesses the compliance, control effectiveness, and work efficiency of each work unit. The assessment activities by internal audits are conducted periodically using sampling and risk based audit techniques. The risk management

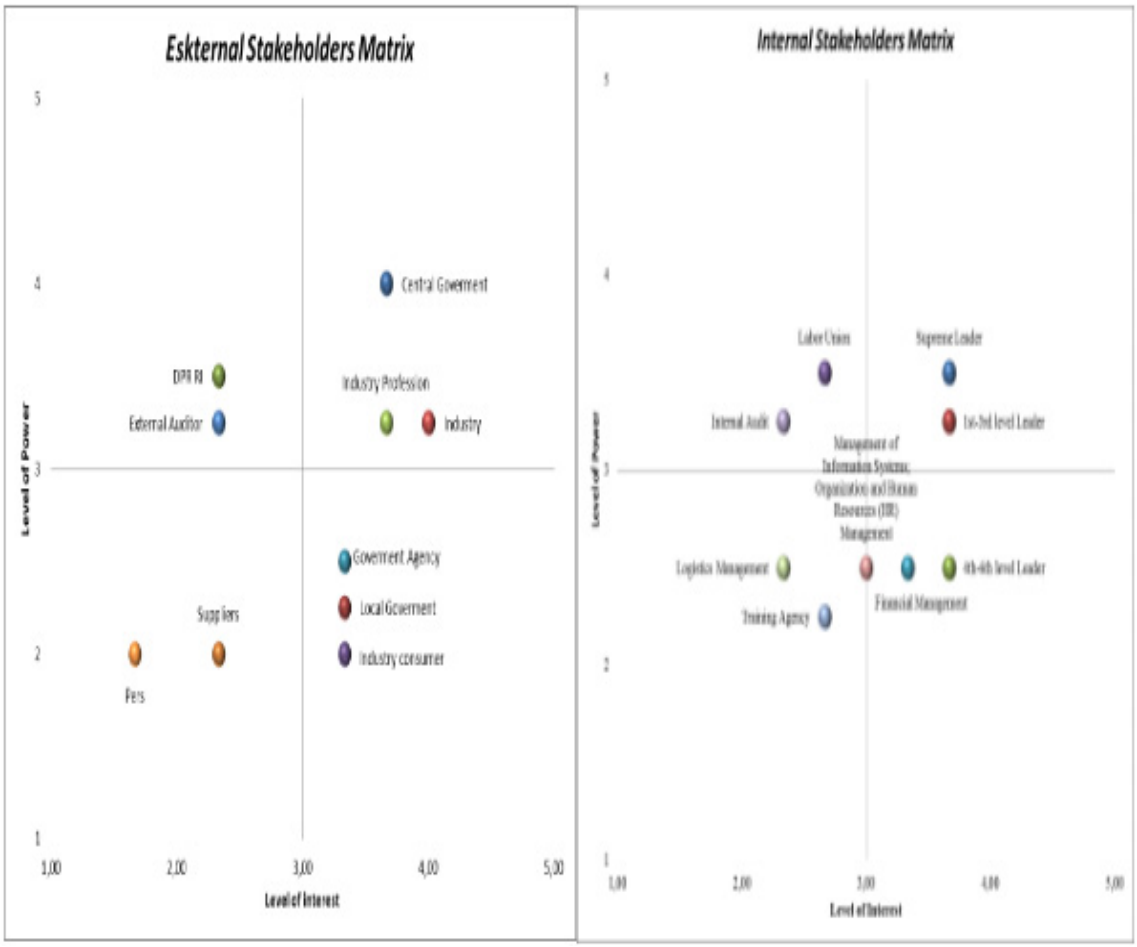

Figure 3
Eksternal and Internal Stakeholders Matrix

unit formulates the risks that will be faced by the organization for the next one year. Risk Management unit is assisted by the risk officer in each work unit. In addition to participating in organizational risk formulation, the risk officers also carry out risk identification of work units and monitor risk mitigation in their work units. The risk management unit also coordinates self assessment control and quality assurance in each work unit assisted by the Quality Officer in each work unit.

Risk management in this organization prioritizes risk management with a very high level of risk impact. This can be seen from the matrix policy assessing the level of risk set by the organization for use at the internal of the organization. The risk assessment matrix assesses all risks to be very high and becomes a top priority when these risks have a very high risk impact even though these risks are very rare.

The organization also applies a zero tolerance policy for fraud risks. There is no fraud risks who have a low and very low risk level. All fraud risk in this organization has a level of likelihood and impact with a level of "Medium", "High", or "Very High" (Figure 2).

Currently, fraud handling has been carried out through whistle blowing systems, gratuity control programs, LHKPN (report on the assets of state officials) management, integrity surveys, and investigative / prosecution audits. In addition, fraud risk management will also be applied to this organization next year.

Research Methodology

To identify inherent fraud risk, the steps to be taken are:

1) Conduct an analysis of internal and external contexts
2) Identifying fraud schemes in each of the main tasks
3) Calculating the level of likelihood of risk events
4) Calculate the level of significance / im-

Table 2
Fraud Schemes on Organizations

Fraud Potential Scheme based on ACFE grouping: 2018a		Initial Risk
Corruption	Conflict of interest in procurement	R.1.1
	Conflict of interest in supervisory	R.1.2
	Conflict of interest in licensing	R.1.3
	Conflict of interests in external regulatory	R.1.4
	Conflict of interests in internal arragement	R.1.5
	Conflict of interests in Enforcement/inspection	R.1.6
	Bribes by third parties	R.1.7
	Bribes by internal parties	R.1.8
	Illegal gratuity by 3rd party	R.1.9
	Illegal gratuities by internal parties	R.1.10
	Extortion to 3rd party	R.1.11
	Extortion to internal parties	R.1.12
Asset Misappropriation	Misuse of assets	R.2.1
	Theft of assets	R.2.2
	Theft in assets distribution	R.2.3
	Fictitious payments	R.2.4
Financial Statement Fraud	Improper assets valuation	R.3.1
	Improper revenues valuation	R.3.2

Source: Data Process

Table 3
Inherent Fraud Risk Level

Initial Risk	Likelihood Level	Significance Level	inherent fraud risk Level
R.1.1	4	3	High
R.1.2	3,5	5	Very High
R.1.3	4	5	Very High
R.1.4	4	5	Very High
R.1.5	5	3	High
R.1.6	4	5	Very High
R.1.7	5	4	Very High
R.1.8	4	3	High
R.1.9	5	4	Very High
R.1.10	4	3	High
R.1.11	5	5	Very High
R.1.12	4	3	High
R.2.1	4	3	High
R.2.2	4	3	High
R.2.3	3	3	Medium
R.2.4	4,5	3	High
R.3.1	3	5	Very High
R.3.2	3,5	5	Very High

Source: Data Process

pact of risk
5) Mapping the level of inherent fraud risk in the heat map

4. RESEARCH RESULT AND DISCUSSION

Eksternal and Internal context

Assumptions:

each work unit has the following general tasks:

1) All work units have the authority to procure goods/services related to their respective main tasks. For this reason, all work units have the potential for fraud in the scheme of conflict of interest in the procurement of goods / services, bribes by third parties, illegal gratuities by third parties, extortion to third parties, and payments to fictitious vendors.
2) All work units have the authority to manage their assets and inventories. For this reason, all work units have the potential for misuse of asset and theft in assets.
3) All work units manage risk in their respective work units, for which all work units have the potential for fraud in the scheme of conflict of interest in internal arrangements.

From each fraud scheme that has been identified, the possibility of fraud risk is calculated by considering several assumptions as follows:

1) Based on the zero tolerance policy, the level of occurrence for fraud risk is "Medium", "High", and "Very High".
2) The parameters of the likelihood level of fraud scheme based on the percentage of the appearance of fraud schemes in the work unit are as follows:
   a) Likelihood of fraud risk schemes administered by all work units has a "Very High" level of occurrence (5)
   b) Likelihood of fraud risk schemes administered by 50% <work units <100% have a level of "High" occurrence (4)
   c) Likelihood of fraud risk schemes administered by 50% of work units

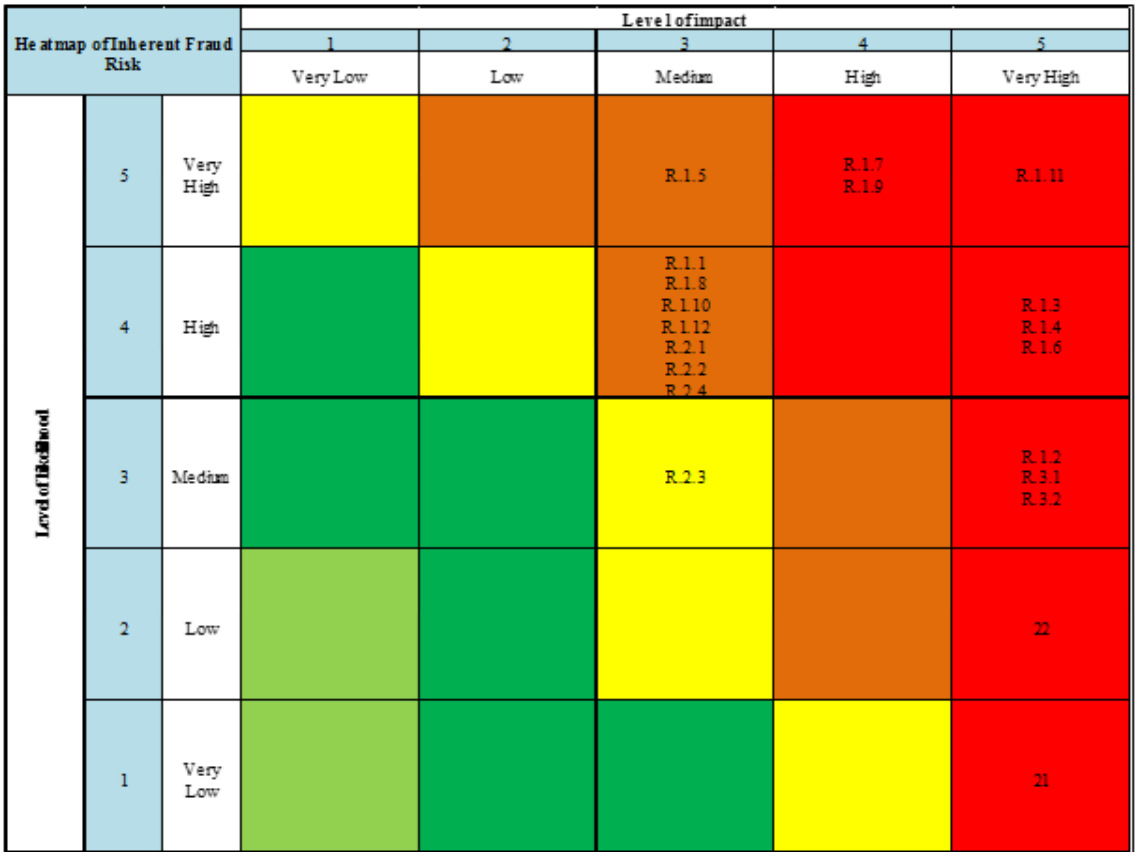

Figure 4
Inherent Fraud Risk Level

or lacking have a level of "Medium" occurrence (3)

3) The parameters of the likelihood level of fraud scheme based on the party implementing the fraud scheme in the work unit are as follows:
   a) Likelihood of fraud risk schemes carried out by internal stakeholders in quadrant I and / or II has a "Very High" level of occurrence (5)
   b) Likelihood of fraud risk schemes carried out by internal stakeholders in quadrant III has a level of "High" occurrence (4)
   c) Likelihood of the fraud risk scheme carried out by internal stakeholders in quadrant IV has a level of "Moderate" occurrence (3)
4) The level of total likelihood is the average of the likelihood level based on the percentage of the appearance of fraud schemes in work units with the likelihood level based on the party implementing the fraud scheme in the work unit.

The significance level of the fraud risk is carried out in order to see how much impact the risk will cause if the risk of fraud occurs. For each fraud scheme that has been identified, the significance level of the fraud risk can be calculated by considering the following assumptions:

1) Based on the zero tolerance policy, the significance level for fraud risk is "Medium", "High", and "Very High".
2) Significance of fraud risk schemes that directly affect external stakeholders in the first and second quadrants have a "Very High" level of occurrence (5)
3) Significance of fraud risk schemes that directly affect external stakeholders in quadrant III have a "High" level of occurrence (4)
4) Significance of fraud risk schemes that directly affect external stakeholders in quadrant IV have a level of "Moderate" occurrence (3)
5) Significance of fraud risk schemes that

directly affect the organization's operational activities have a level of "Moderate" occurrence (3)

5. CONCLUSION

Factors that can influence inherent fraud risk in an industrial supervision are as follows: (1) Main tasks of the work unit in the organization. (2) Organizational context. (3) Percentage of appearance of fraud schemes in work units. (4) Executor of work in the work unit tasks. (5) Level of influence of external stakeholders. The order of the main tasks with the number of fraud risk schemes can be presented as follows. The main task of information system management has the most fraud risk scheme among other main tasks, this is because of the duties and authority in managing information systems also contain tasks related to the procurement of goods and services. In addition, the

Table 4
Fraud Schemes Based On Main Task

Number	Main Task	Count of Fraud Schemes
1	Management of Information Systems	10
2	Logistics Management	9
3	Industrial Supervisory	6
4	Industrial Licensing	4
5	Integrated Supervisory	4
6	Industrial Investigation	4
7	Internal audit	4
8	Industrial regulatory	3
9	Integrated regulatory	3
10	Consumer Protection	3
11	Human Resources (HR) Management	3
12	Financial Management	2
13	Legal	2
14	Training Agency	2
15	Consumer education	1
16	Organization Management	1
17	Strategic Management	1
18	Risk Management	1

Source: Data Process

Table 5
Fraud Schemes Based On Work Unit

Number	Work Unit	Count of Fraud Schemes
1	Industrial Regulations and Supervision	13
2	Internal Audit and Risk Management	12
3	Organization and Human Resources (HR) Management	11
4	Integrated Regulation and Supervision	10
5	Strategic and Logistics Management	10
6	Management of Information Systems	10
7	Industrial Investigation	9
8	Financial Management	9
9	Legal Unit	9
10	Consumer Education and Protection	8
11	Training Agency	8

Source: Data Process

management of information systems must also manage and distribute information systems in the organization. The Industrial Regulatory and Monitoring Unit has the highest number of potential fraud schemes compared to other work units. This is because this unit carries 6 main tasks, namely related to industrial regulation, industrial supervision, industrial licensing, financial management, asset management, and risk management (Table 5).

Implication

Identification of inherent fraud risk is the first step in implementing fraud risk assessment. Thus, the organization needs to continue at the stage of assessing internal control for each of the main tasks in order to obtain the level of residual fraud risk. The residual risk level for fraud is needed by the organization to determine the appropriate handling in order to avoid fraudulent schemes.

Suggestions

Some of the options that the organization can choose in order to minimize fraud risk as described above are as follows: (1) Reducing residual risk with reliable internal controls. (2) Reducing inherent fraud risk: centralizing the implementation of logistical tasks, and / or restructuring organizations, especially the Industrial Regulatory and Supervision unit

Limitations

This study has limitations that require improvement and development in subsequent studies. Some limitations of this study include: (1) This study assesses inhrent fraud risk in the organizational structure without distinguishing the authority of each leadership level. The suggestion for further research is to carry out a more detailed assessment of inherent fraud risk for each official's authority and executor in it. (2) In the organizational structure, the industrial regulation and supervision unit is divided into 3 units in accordance with the type of industry that they supervise. This study does not distinguish cultures from each type of industry. The culture of each type of industry can also influence inherent fraud

Table 6
Inherent Fraud Risk Priority List

Number	Fraud Schemes	Level of Inherent Fraud Risk
1	Extortion to 3rd party	Very High
2	Conflict of interest in licensing	Very High
3	Conflict of interests in external regulatory	Very High
4	Conflict of interests in Enforcement/inspection	Very High
5	Conflict of interest in supervisory	Very High
6	Improper assets valuation	Very High
`7	Improper revenues valuation	Very High
8	Bribes by third parties	Very High
9	Illegal gratuity by 3rd party	Very High
10	Conflict of interests in internal arragement	High
11	Conflict of interest in procurement	High
12	Bribes by internal parties	High
13	Illegal gratuities by internal parties	High
14	Extortion to internal parties	High
15	Misuse of assets	High
16	Theft of assets	High
17	Fictitious payments	High
18	Theft in assets distribution	Medium

Source: Data Process

risk in this organization. Thus, for further research, it can conduct more in-depth research related to the cultural aspects of each industry that are monitored. (3) This research stops at the stage of identifying inherent fraud risk. The risk level in the results of this study cannot be used in the risk handling process. The next step that needs to be assessed is the effectiveness of internal control of each process in the main task. The assessment of the internal control effectiveness can be done by audit techniques and self assessment by each related work unit. Suggestions for further research is to assess the effectiveness of internal controls in this organization, so that the level of residual risk and the appropriate form of treatment for each fraud risk can be assessed.

6. REFERENCES

ACFE. (2008). *Fraud Examiners Manual.* The Association of Certified Fraud Examiners.

ACFE. (2016). *Fraud Prevention and Deterrence.* The Association of Certified Fraud Examiners.

ACFE. (2018a). *Report to the Nations.* Texas: The Association of Certified Fraud Examiners.

ACFE. (2018b). *Report to the Nations; Asia-Pacific Edition*. Texas: The Association of Certified Fraud Examiners.

Beasley, M., Carcello, J., & Hermanson, D. (2001). Top 10 Audit Deficiencies . *Journal of Accountancy*.

CIMA. (2009). *Fraud Risk Management: A Guide to Good Practice.* London: Chartered Institute of Management Accountants.

Cohen, L., Felson, M., & Land, K. (1980). Property Crime Rates in the United States: A Macrodynamics Analysis. *American Journal of Sociology*.

COSO. (2013). *Internal Control - Integrated Framework.* Commitee of Spronsoring Organisations of the Treadway Commission.

COSO. (2016). *Fraud Risk Management Guide.* AMERICA: COSO.

Eden, C., & Ackermann, F. (1998). *Making Strategy: The Journey of Strategic Management.* London: Sage Publications.

Guercio, J., Rice, E., & Sherman, M. (1988). Old Fashioned Fraud by Employees is alive and Well: Result of a Survey of Practicing CPAs. *The CPA Journal*.

Hofstede, G. (1983). The Cultural Relativity of Organizational Practices and Theories. *Journal of International Business Studies*.

Hofstede, G. (1993). Cultural Constraints in Management Theories. *Academy of Management Executive*.

Hofstede, G., & Bond, M. (1988). The Confucius Connection: From Cultural Roots to Economic Growth. *Organizational Dynamic*.

Holmes, S. A., Strawser, J. W., & Welch, S. T. (2000). Fraud In The Govermental and Private Sectors. *Journal of Public Budgeting, Accounting & Financial Management*.

IIA; AICPA; ACFE. (t.thn.). *Managing The Business Risk of Fraud: A Practical Guide.*

ISO 31000. (2018). *Risk Management - Guidelines.* Geneva: International Standard Organization.

Mann, K. (1992). White-Collar Crime and te Poverty of the Criminal Law. *Law and Social Inquiry*.

Maxfield, M. (1987). Lifestyle and Routine Activities of Crime. *Journal of Quantitative Criminology*.

Miller, T. C., Cipriano, M., & Ramsay, R. J. (2012). Do auditors assess inherent risk as if there are no control? *Managerial Auditing Journal*.

Seidman, J. (1990). A Case Study of Employees Frauds. *The CPA Journal*.

Shailer, G., Wade, M., Willett, R., & Yap, K. L. (1998). Inherent Risk and Indicative Factors: Senior Auditors' Perceptions. *Managerial Auditing Journal*.

Shapiro, S. (1990). Collaring the Crime, Not the Criminal: Reconsidering the Concept of White-Collar Crime. *American Sociological Review*.

Wheeler, S., & Rothman, M. (1982). The Organization as Weapon in White-Collar Crime. *Michigan Law Review*.