ATLANTIS PRESS

Advances in Economics, Business and Management Research, volume 127

Annual International Conference on Accounting Research (AICAR 2019)

Influence Analysis of Financial Audit Ethics in the Merger and Acquisition Process Toward White Collar Crime

Ekawahyu Kasih*, Ruslaini Ruslaini
Founder of STIE Kasih Bangsa
Jakarta, Indonesia
*dr.kasih1@gmail.com

***Abstract*—White-collar crime, along with the use of information technology, has grown rapidly in committing crimes, including cyber-crime and non-compliance with laws and regulations especially regarding the making of financial statements that are not in accordance with the prevailing laws and regulations. The situation inevitably may harm investors, creditors and other stakeholders and often happens in the merger and acquisition process of the company. This study uses descriptive qualitative method to elaborate and explain the phenomena. Research findings of The International Ethics Standards Board for Accountants (IESBA) issued on July 14, 2016 has been adopted by more than 100 countries to become a benchmark for conducting corporate financial audits to minimize non-compliance with laws and regulations. Then, The Foreign Corrupt Practices Act (FCPA) has succeeded in reducing the criminal acts of corruption committed by the public, private sector, companies and individuals living in America and corruption, including bribery to foreign government officials. Similarly, the Public Company Accounting Oversight Board (PCAOB, 2015) has been able to go hand in hand with IESBA in combating criminal acts in presenting financial statements that violate both immaterial and material laws and regulations affecting the financial statements. Conclusion of the study is financial audit ethics in the merger and acquisition process must be applied and become part of government regulations in combating white collar crime so that there are no losses and large impacts for companies, investors, creditors that in turn will affect one country's economy.**

Keywords: financial audit ethics, auditor, white collar crime

I. INTRODUCTION

Management of a business is good if it is able to get profit consistently which does not violate business ethics and prevailing law where the business is operating. In business ethics education and training both in corporate and college, there are often faced with the dilemma between profit as a company's goal and business ethics and business law even though all managers are always willing to do business well by maintaining their balance in business operations.

This paper emphasizes business ethics in the context of corporate financial audits. It is also can be of business and non-business situations. Many parties unfortunately allow the occurrence of violations of ethics and law in business, especially the irregularities audit process, and the results of corporate financial audits that benefit one party and harm many parties. Often it also happens long before audited financial statements are published there has been negotiation and conditioning between corporate managers and the auditors, due to the close relationship between them. The same can also happen during due diligence in the merger and acquisition of a company. There can be many violations of ethics and even law violations either done by the company without the auditor's knowledge or occur due to collusion between the company and the auditors.

White-collar crime through information technology (cyber-crime) has caused great harm and impact for companies, investors, creditors and other stakeholders. Often various white-collar crimes in the new company are caught after an audit by a professional independent auditor that firmly upholding the code of conduct of the audit.

Formulation of the problem:

- How does a white-collar crime in the company's due diligence process relate to corporate mergers and acquisitions?
- What is the role of information technology development against white-collar crime?

II. LITERATURE REVIEW

A. White Collar Crime in the Company's Due Diligence Process Relates to Company's Mergers and Acquisitions

The balance sheet of companies in the USA shows excess cash so they look for other business opportunities by utilizing the excess cash in the interest of shareholders. Currently the business environment in the USA is less conducive to increasing profits through increased sales. This is due to increased unemployment rate, declining purchasing power, rising commodity prices and tightening credit disbursement from financial institutions and banks due to the crisis that hit Europe. One way to increase the value of a company is through the acquisition of the company. By merger and acquisition then hopefully the company can:

- Strengthen market share position.
- Increase economies of scale.
- Develop new markets.

This process can provide the advantages of new skills, synergy, knowledge and technology that enable companies to be more efficient and effective. In the process of due diligence in the framework of mergers and acquisitions, the most feared by the acquiring party is corruption in the form of bribery by the company to be acquired to the auditor who performs the due diligence so that it is contrary to the Foreign Corrupt Practices Act (FCPA).

Bribery is a form of corruption that involves giving, offering, requiring, or receiving something of value to influence official action [1]. Another form of bribery in business deals with giving money to influence business decisions. A US company case Information Technology in Latin America has fined $ 2 million for foreign corruption practices (e.g. FCPA). Even though it is small comparing to other fines resulting from FCPA violations, USA firms spend $ 26 million to investigate, report and correct such violations.

Good corporate management must understand about FCPA. In general, FCPA does not permit US citizens and public or private companies , foreign companies listed on US stock exchanges or foreign nationals living in the United States to give money or other valuables directly or indirectly to foreign officials to retain or obtain business.

The scope of bribes in the FCPA involves the delivery of valuables goods to foreign officials in order to maintain or obtain business. The meaning of the provision of a bribe of valuable goods is that can be cash, equivalent to cash, prizes, discounts, facilities, equipment, food, beverage, entertainment, lodging, transportation, insurance benefits and promise work. Here, the so-called foreign officials are not only government officials but also include government officials in the field of supervision. Then, what is meant by maintaining or obtaining business is not solely related to foreign government contracts.

In conducting mergers and acquisitions, companies that will merge and acquire should use forensic accountants during the due diligence process to look for any possible crimes and at the same time perform accurate analysis to obtain accurate reports. The following is a list of questions that can be submitted to the company to be acquired to avoid the risk of errors in mergers and acquisitions as follows:

Risk-assessment questions for the target company [2]:

- Does the company in a country that has anticorruption legislation?
- In what countries does the company conduct business?
- Do you have anticorruption legislation?
- Is the company in a highly regulated business?
- Does the company sell deal with foreign governments?
- To what extent does the company supply products to foreign government or government-controlled entities?
- Are there compliance programs in place?
- If there are compliance programs in place, what is the extent of the programs?
- Have the compliance program policies been distributed to all employees and agents?
- What extent are the compliance policies regularly enforced?
- Are there records of enforcement of compliance policies maintained?
- Has the company come under suspicion of corruption?
- Has the company been publicly sanctioned?
- Have company directors or key managers come under suspicion of corruption?
- Have company directors or key managers been publicly sanctioned?
- Have background checks been performed on agents and key members of management to identify possible government links?
- Have background checks been performed on customers to identify possible government links?
- Does the company conduct business through third parties?
- If the company conducts business through third parties, what does the company use third parties?
- What are the amounts of sales-related commissions, retainers, and expenses paid to third parties?
- Does the company have written agreements for international agents in regard to FCPA and anticorruption?
- Have the company's competitors been the subject of an FCPA investigation?
- What is the typical value of sales to customers?
- To what extent does the company use gifts, hospitality, and / or travel services for sales and marketing?
- What does the company do for business?

III. METHODS

This study uses descriptive qualitative methods where secondary data were collected from published international journals.

IV. RESULTS AND DISCUSSION

A. Cyber Crime and White Collar Crime

White collar crime has become the epidemic of the world. White-collar crime is growing rapidly along with the use of information technology in crime (cyber-crime). Cyber-crime is defined as the use of computers to unlawfully gain resources or

goods or compromise other entities at the expense of, alteration, or damage to software, hardware or data. Manifestation of white-collar crime can be a traditional form of corporate financial report engineering, bribery, extortion, pricing, forgery, embezzlement, insider trading, securities crime, counterfeiting, money laundering, kick back, money laundering, salary fraud, tax evasion.

With the development of information technology, the white-collar crime develops, including the theft of identity data, cyber-crime, credit card crimes, telematics crimes, and others. The following are things to do in the prevention and detection of white-collar crime as follows:

Checklist for prevention [3]:

- Implement an effective system of separation of duties.
- Establish internal controls for input data.
- Establish internal controls for data output.
- Establish internal controls for system modification.
- Protect passwords through an effective password administration.
- Do not create group passwords.
- Revoke passwords when employees change job functions.
- Immediately revoke passwords of terminate employees.
- Change passwords at frequent intervals.
- Use passwords with at least eight characters, including numbers and upper-and lowercase letters.
- Educate employees regarding information security.
- Create a security policy.
- Establish controls to guard against access by third parties.
- Establish a code of ethics.
- Use vigorous disciplinary actions against offenders.
- Perform software maintenance in a supervised environment.
- Check employee references.
- Use vulnerability scanning tools to look for system oversight and vulnerabilities.
- Establish special authenticated measures for wireless networks.
- Diligently enforce policies regarding passwords, access, and authorization.
- Establish external and internal guidelines for communication if the system is compromised.
- Regularly scan the system for weaknesses, unauthorized usage anomalies, and any signs of misuse.

Software Applications for the Detection of WCC [3]:

- Searching for duplicate payments.
- Comparing vendors to employees who are also vendors.
- Searching for duplicate or missing check numbers.
- Scanning for vendors with post office box addresses.
- Scanning for new vendors with a high level of activity.
- Scanning for vendors with the same mailing address.
- Identifying vendors that have more than one mailing address.
- Scanning for unapproved vendors.
- Scanning for fraudulent checks.
- Scanning for invoices with no purchase order number.
- Scanning for transactions that fall just below financial control.
- Employing ratio, vertical, and horizontal analysis.
- Identifying unusual relationships by using correlations analysis.
- Scanning for excessive cash transactions.
- Scanning for excessive use of exchange items.
- Scanning for significant change in bad debt write off.
- Scanning for the recurrence of same amounts.
- Scanning for sudden activity in dormant accounts.

Cybercrime attacks have targeted the public and private sectors. In 2013 the American government has enacted a better law against cyber-crime. Most experts believe that the best solution to cyber-crime is good coordination between the public and private sectors in the fight against cybercrime. The things that need to be done are:

- Realizing that the threat of cyber-crime is real.
- Conducting a rigorous risk assessment of cyber-crime.
- Addressing and mitigating major risks.
- Constantly communicating with an agency specializing in cyber-crime.

B. The International Ethics Standards Board for Accountants (IESBA)

The International Code of Ethics for Accountants (IESBA) published on July 14, 2016, is to address non-compliance with laws and regulations has been adopted by more than 100 countries including Canada and Mexico. With the implementation of IESBA standards it is expected white-collar crime related to the work of accountants. Auditor and financial management company to present financial statements that are not in accordance with the actual circumstances can be avoided. IESBA ethical standards have similarities and

differences with PCAOB (Public Company Accounting Oversight Board).

There are 3 specific differences: standard coverage, initial investigation process, recommendations on "whistle blowing ".

1) Standard coverage:

a) IESBA standard coverage:

- Crime, corruption and bribery.
- Money laundering, terrorism financing, and crime proceeds.
- Securities and transaction markets.
- Financial institutions and banking.
- Taxes and pension payments obligations.
- Environmental protection.
- Public health and safety.

b) PCAOB standard coverage: The PCAOB auditing standards (AS 2405) of Illegal Acts by Clients are narrower than IESBA ethics standards, where PCAOB is only for the material effects of financial statements, so that if illegal actions are not material in the financial statements the auditor has no obligation to disclose based on PCAOB.

c) Initial investigation process: The steps IESBA recommended when found NOCLAR (Non Compliance with Laws and Regulation) are:

- Gain an understanding of the deed and its consequences and consultation with companies, professional bodies or legal institutions.
- If NOCLAR has been found, it should be immediately discussed with appropriate management level or with responsible individuals including internal auditors.
- Determine whether management and those who are responsible understand their responsibilities, and seek advice from legal institutions.
- Comply with applicable laws and auditing standards including taking into account the conclusion of non-compliance with laws and regulations in the conclusion of the audit report.
- If the involved is part of the audit group, then non-compliance with laws and regulations should be of interest to the partners.

Steps recommended by PCAOB in the initial investigation:

- Obtain an understanding of the actions and consequences and other information necessary to evaluate the effects of financial reports, consultation with responsible management levels.
- If management is dissatisfied with the auditor for non-illegal conduct, consultation with the client's legal department, uses additional procedures if necessary to gain an understanding of the likelihood of illegal acts.
- If the auditor's conclusion has been illegal then consideration of the impact on the financial statements and other aspects of the audit.
- Audit committees should be notified.

In some cases, the two standards above require both investigation and consultation. PCAOB investigations are terminated if the impact on the financial statements is immaterial. However, IESBA investigations will continue if non-compliance with laws and regulations have not been resolved thoroughly even if they do not have a material impact on the financial statements.

d) Advanced action and " whistle blowing ": If a major investigation has found noncompliance with laws and regulations and is not resolved properly and thoroughly then do whistle blowing as an alternative.

C. IESBA and Whistle Blowing

If the conclusion is satisfactory, then the problem can be closed and no follow-up action is required. However, if the professional accountant lost confidence in the integrity of management and the responsible party, the accountant can downloading resign. Another option is to be a whistle blower.

D. PCAOB Standards and Whistle Blowing

PCAOB standards for illegal acts do not permit openly disclosed matters concerning client confidential information. If the accounting professional makes the Decision to disclose client confidential information and become a whistle blower, then the action is contrary to the PCAOB standard.

If a major investigation has found noncompliance with laws and regulations and is not resolved properly and thoroughly then do whistle blowing as an alternative.

V. CONCLUSION

White-collar crime has grown very rapidly along with the use of information technology in committing crimes including cyber-crimes and non-compliance with laws and regulations especially regarding the making of financial statements that are not in accordance with the actual facts that may harm investors, creditors and other stakeholders. This often happens in the merger and acquisition process of the company. The International Ethics Standards Board for Accountants (IESBA) issued on July 14, 2016 has been adopted by more than 100 countries to become a benchmark for conducting corporate financial audits to minimize non-compliance with laws and regulations.

The Foreign Corrupt Practices Act (FCPA) has succeeded in reducing the criminal acts of corruption committed by the public, private sector, companies and individuals living in America and corruption, including bribery to foreign government officials.

Similarly, the Public Company Accounting Oversight Board (PCAOB, 2015) has been able to go hand in hand with IESBA in combating criminal acts in presenting financial

statements that violate both immaterial and material laws and regulations affecting the financial statements.

REFERENCES

[1] J.T. Wells, The Computer and Internet Fraud Manual. Association of Certified Fraud Examiners, Inc., 2004

[2] J.R. Byington and J.A. McGee, M & A Due Diligence: How to Uncover Corruption. Wiley Periodicals, Inc., vol. 23, pp. 65-70, 2012.

[3] J.A. McGee and J.R. Byington, "Checlists: Prevent White-Collar Computer Crime," Wiley Periodicals, Inc., vol. 23, pp. 49-52, 2012.