International Journal of Accounting and Taxation
June 2020, Vol. 8, No. 1, pp. 44-54
ISSN: 2372-4978 (Print), 2372-4986 (Online)

Published by American Research Institute for Policy Development
DOI: 10.15640/ijat.v8n1a6
URL: https://doi.org/10.15640/ijat.v8n1a6

The Audit Investigation and Accounting Forensicin Detecting Fraud in Digital Environment

Prastika Suwandi Tjeng[1] & Rina Nopianti[2]

Abstract

A forensic accountant helps organizations or individuals primarily to provide management support in the form of reports to detect fraud and support litigation, primarily through expert witness testimony. The objectives to be achieved in this study are to explore how investigative and forensic accounting audits are applied in detecting fraud in the digital environment and to find out why investigative audits and forensic accounting in detecting fraud in the digital environment need to be applied. Researchers conducted a library study by collecting several economic journals and books relating to the problem under study. The data collection method in this research is done by interpreting and analyzing qualitative data. The results of this study indicate that forensic accounting in detecting fraud in the digital environment can be done by computer forensic and investigations that must be done by making copies of the entire log data, making fingerprints from numerical data, making fingerprints from copies, making master list hashes and documenting data that has been done.

Keywords: Digital Environment, Forensic Accounting, Fraud, Investigative Audit.

Introduction

The high level of corruption has become a powerful driver for the development of forensic accounting practices in Indonesia. Forensic accounting is needed because of the potential for fraud that is capable of destroying the government, business, education, departments and other sectors. Fraud occurs because of low corporate governance, weak enforcement, weaknesses in the field of law enforcement, accounting standards and others consistent with the level of corruption and weaknesses in the administration of the country. Lately, cases of fraud that often occur in Indonesia, namely cybercrime, or commonly called as white-collar crime. Lately, cybercrime has increasingly increased. The handling of cybercrime cases is still quite tricky because the technology in Indonesia is still inadequate, and the lack of knowledge of digital techniques. The methods and methods used to manipulate companies are numerous, and the possibility of detecting all fraud through a computer is just a dream. Only a small number of cases that occur can be revealed while cases that occur, the number is astonishing.

In addition to cybercrime, white-collar crime is a crime that is rife in Indonesia. White-collar crime is limited to crimes committed within the scope of their office and therefore, does not include crimes of murder, adultery, rape, and others. That is generally not within the scope of the activities of white-collar criminals. Some of the examples of a white-collar crime that occurred in Indonesia is the Century Bank bailout case that began in October 2008 in which the perpetrators of these crimes are officials who have authority in Century Bank. Another example that has recently happened in the case of Jiwasraya and Asabri Insurance which has a systemic impact. Furthermore, until now, these cases have not been resolved. One of the causes of the problematic detection of fraud in Indonesia is due to the continued development of forensic accounting and the absence of experts who can disclose the fraud so that handling is delicate. Accounting graduates who work as accountants or auditors, like it or not, must understand forensic accounting. Therefore, the discipline of accounting is required to make changes and follow the trend of current problems, especially those related to fraud issues. That way, academics can be more responsive to fraud cases both in the digital environment and outside the digital environment that often occurs as an indication of corruption in this country.

[1] Program studiAkuntansi, Universitas Multimedia Nusantara, prastika.suwandi@lecturer.umn.ac.id
[2] Program studiAkuntansi, Universitas Bina Bangsa. E-mail: rina.nopianti@binabangsa.ac.id

Literature Review

1. Audit Investigation

Over time, the development of forensic accounting has become more sophisticated, involving one more area, namely auditing. The growing complexity of business and the increasingly opening up of business and investment opportunities leads to a higher risk of fraud. Referring to various cases, both inside and outside the country shows that fraud can occur anywhere. In order to minimize losses due to fraud and improve the control system, if there are strong indications of fraud, the company is expected to take appropriate steps to conduct an investigative audit (Scotland, 2017). Conducting an investigative audit is based more on the mindset that in order to expose a fraud the auditor must think like the perpetrators of fraud themselves, by basing the implementation of procedures established at the planning, implementation, reporting and follow-up stages of the audit (Rapp, 2010).

Auditors must have the ability to prove the existence of fraud that has occurred and previously indicated by various parties. The auditor must be sensitive to all things that are unnatural whether it is felt too big, too small, too often, too low, too much, too little, or an odd impression. Auditors must be able to communicate in their "language". The auditor must also have the technical ability to understand financial concepts and the ability to conclude. Furthermore, it is also imperative for auditors to simplify financial concepts so people, in general, can understand what they mean. Investigative auditors are "a combination of lawyers, accountants, criminologists and detectives (or investigators)"(Justenhoven, Sechser, & Loitz, n.d.).

1.1 Definition of Investigative Audit

An investigative audit is a form of audit that aims to identify and uncover fraud or crime using approaches, procedures or techniques commonly used in an investigation or investigation of a crime (Imoniana, 2013).

An investigative audit is similar to the term Fraud Examination as referred to in the Fraud Examination Manual published by the Association of Certified Fraud Examiners (ACFE). According to the manual of the fraud examiners, what is meant by an investigative audit is the methodology for resolving fraud allegations from inception to disposition. More specifically, fraud examination involves obtaining evidence and taking statements, writing reports, testifying findings and assisting in the detection and prevention of fraud(Reurink, n.d.).

1.2 Difference between Financial Audit and Investigative Audit

There are several differences between a financial audit and an audit investigation, namely:

1. Basis of Audit Implementation; the basis of conducting an investigative audit is a request from the investigator to detect possible fraud. Besides, an investigative audit can also be conducted based on complaints from the public about suspicion of fraud and from audit findings that lead to the possibility of fraud obtained from previous financial audits.
2. Auditor's responsibility; in financial audits, audits are responsible on behalf of the audit institution or the Public Accounting Firm (KAP) where the auditor works. In an investigative audit, the auditor is responsible for the designated personal name, because if the statement in a court hearing is a false statement, the auditor in question will be subject to sanctions.
3. Audit Objectives; the purpose of the financial audit is to find out the client's financial statements by generally accepted accounting principles. An investigative audit aims to help the investigator to make the case clear by looking for the evidence needed to support the prosecutor's indictment.
4. Audit Techniques and Procedures; in financial audits, audit procedures and techniques used refer only to auditing standards, while investigative audits refer to auditing standards as well as the investigator's authority so that more extensive audit techniques can be used.
5. Implementation of the Audit Planning and Implementation Principle; the financial audit uses scepticism professionalism, while investigative audits besides using scepticism professionalism also use the principle of presumption of innocence.
6. Requirements of the Audit Team; auditors, must master accounting and auditing issues, while in investigative audits, auditors must also know the applicable legal provisions in addition to mastering accounting and auditing issues.
7. Audit Report; the auditor's opinion regarding the suitability of the financial statements with accounting principles generally applies. In an investigative audit, states who is responsible and involved in fraud cases handled, but still applies the principle of presumption of innocence.

1.3 The purpose of the investigation

The purpose of the investigation are some of them (Beneish et al., 2011):

1. Dismiss management. The aim is as a stern rebuke that management is unable to account for its fiduciary obligations.
2. Examine, collect and assess enough and relevant evidence. The aim will be to emphasize the acceptance of evidence as evidence to convince a judge in court.
3. Protect the reputation of innocent employees.
4. It is finding and securing relevant documents for investigation.
5. Find the embezzled assets and seek recovery from the losses incurred.
6. They are ensuring that the perpetrators of crime cannot escape their actions.
7. It wiped out all employees of a criminal.
8. It is ensuring that the company is no longer the target of pillaging.
9. Determine how the investigation will proceed.

1.4 Principles of Investigative Audit

The following principles based on experience and practice can be used as guidelines for investigators in each situation as follows (Beneish et al., 2011):

1. The investigation is the act of searching for the truth by paying attention to justice and based on the provisions of the applicable legislation.
2. Investigation activities include the use of evidence sources that can support the facts in question.
3. The investigator collects facts in such a way that the evidence obtained can provide his conclusions.
4. Information is the breath and blood of the investigation so that the investigator must consider all possibilities to obtain information.
5. Observations, information and interviews are an essential part of an investigation.
6. The perpetrators of crime are humans; therefore if they are treated as befits humans, then they will also respond like humans.

1.5 Axiom of Investigation Audit

There are three axioms in conducting an investigative audit (Reurink, n.d.):

1. Fraud is always hidden. Fraud, in this case, hides all aspects that might be able to direct other parties to find the occurrence of fraud. The parties involved closed their rotten meetings. The method of concealing fraud is so neat that even an experienced fraud inspector or investigator can be fooled.
2. Perform interactive proof. An auditor must consider whether there is evidence that could incriminate a suspect who has never committed fraud. Moreover, conversely, the auditor must also be able to consider whether evidence that does not incriminate a person has committed fraud.
3. Fraud happens to be the court's authority to decide. In investigating fraud, the investigator only makes guesses about whether a person is guilty or not based on the evidence he has collected. However, the fraud existence that occurs can be ascertained if a panel of judges and jury has decided it in court.

1.6 Audit Investigation Methodology

According to the internal audit methodology, a fraud auditor can test or examine several matters relating to the subject of the audit or the work procedures and organization where the fraud is suspected and the person concerned (Justenhoven et al., n.d.). To find answers to fraud without complete evidence, the auditor needs to make certain assumptions. The methodology emphasizes when and how to carry out an investigative of cases that have indications of fraud and have implications for the legal aspects, how to proceed. Investigation checks conducted to reveal the existence of fraud consists of many steps. Because the conduct of an investigative investigation of fraud is related to the individual rights of other parties, the investigation must be carried out after a very adequate and strong reason has been termed as predication.

Prediction is an overall condition that directs or shows the existence of a strong belief based on professionalism and caution from the auditor who has been equipped with training and understanding of fraud, that fraud has occurred, is happening, or will occur. Without prediction, an investigative examination cannot be carried out. This causes dissatisfaction from various circles who think that if an audit institution finds an indication of irregularities in carrying out its financial audit, then the institution can conduct an investigative audit.

The investigation is not necessarily directly carried out because the indications found are generally still very premature so that it requires a little deepening in order to obtain evidence that is strong enough to be carried out investigation investigations. The overall outline of the investigative audit process, from beginning to end, is broken down as follows (News, 2017):

1. Preliminary Information Review
   The examiner carries out: gathering additional information, compiling facts and process events, determining and calculating tentative financial losses, determining tentative irregularities, and preparing initial hypotheses.
2. Planning Investigation Examination
   At the planning stage, the initial hypothesis testing, identification of evidence, determining the place or source of evidence, analyzing the relationship of evidence with related parties, and preparing an investigation program.
3. Implementation
   At the implementation stage: a collection of evidence, physical testing, confirmation, observation, analysis and testing of documents, interviews, refinement of hypotheses and review of working papers.
4. Reporting
   The contents of the report of the investigation audit include elements against the law, facts and processes of the incident, the impact of financial losses due to irregularities/acts against the law, causes of unlawful actions, parties involved in irregularities/actions against the law that occur, and forms of cooperation between the parties involved in irregularities/actions against the law.
5. Follow Up
   At this follow-up stage: the process has been submitted from the audit team to the leadership of the organization and formally subsequently submitted to law enforcement. Submitting a report on the results of an investigative audit is expected to have entered the investigation stage. Regarding testimonies in the proceedings in court, an investigative audit team can be appointed by the organization to provide expert information if needed.

1.7 Investigative Audit Techniques

Audit techniques are the methods used in auditing the fairness of the presentation of financial statements. Audit techniques commonly used in general audits such as (Olukowade & Balogun, 2016):

i. Physical examination. In the usual physical examination is the calculation of cash, valuable paper, inventory, fixed assets, and tangible goods. For this technique, the investigator uses his senses to know or understand something.
ii. Confirmation. Asking for confirmation is asking the other party (of the investigated) to confirm the truth or untruth of information. In an investigation, the investigator must consider whether a third party has an interest in the investigation.
iii. Checking Documents. Document checks are always carried out in every investigation. With technological advances, documents certainly become more extensive, including information that is processed, stored, and transferred.
iv. Analytical Review. Analytical reviews emphasize reasoning, the thought process. With ethical reasoning will lead to an investigator auditor on the description of the fair, proper or proper individual data deduced from the picture obtained globally, thoroughly. Analytical review is based on a comparison between what is faced with what should occur.
v. Request an Explanation of Oral or Written from the Audite. Requests for information must be strengthened or collaborated with information from other sources or strengthened in other ways.
vi. Recalculate. Recalculating is checking the correctness of the calculation. In investigations, the calculations faced are very complex, based on complex contracts or agreements, there may have been changes and renegotiations many times with different officials.
vii. Observe. This technique is also not much different from a physical examination. Investigators also use their senses to make observations.

Only in investigative audits, audit techniques are exploratory, looking for 'arable areas', or probing or deepening. Of the seven audit techniques, in an investigative audit, the emphasis is on analytical review. To get the maximum results of an investigation, a fraud auditor must also master some investigative techniques, including (Olukowade & Balogun, 2016):

1. Incognito or tapping techniques
2. Interview techniques
3. Seducing techniques to get information
4. Understand body language
5. With the help of software

2.2. Forensic Accounting

Forensic accounting arises because of the rapid development of fraud that occurs, to reveal the fraud required knowledge of forensic accounting. The term forensic accounting is a translation of forensic accounting. According to Cannon Webster's Collegiate Dictionary, the meaning of forensics can be interpreted "concerning the court" or "concerning the application of scientific knowledge to legal matters".

The Criminal Procedure Code (KUHAP) article 179 paragraph (1) states: "Everyone who is asked for his opinion as a judicial medical expert or doctor or other experts must provide expert testimony for justice". In practice, other expert groups include accountants or investigative audit executors who provide expert information for justice. However, they are not yet commonly known as forensic accountants.

Initially, in the United States, forensic accounting was used to determine the distribution of inheritance or reveal motives for murder. For the application of accounting to break the law, the term used forensic accounting (not audit). The practice of forensic accounting grew not long after the economic crisis hit Indonesia in 1997. Forensic accounting can have a useful role in enforcing the law in Indonesia, but its role is still not maximal. Currently, the Financial Transaction Reports and Analysis Center (PPATK) is trying to develop forensic accounting which began to develop in Indonesia since the 1997 economic crisis.

2.2.1Forensic Accounting Scope

a. Private Sector Practice

Fraud if associated with weak corporate governance, can occur both in the public sector and in the private sector. The impact of fraud occurs in the corporate sector, that is the share price of the corporation concerned is lower than the market price. This will affect the assessment of investors when making decisions. It is not uncommon for investors to pay premium shares if the company is indicated to want to improve the weaknesses of corporate governance (Olukowade & Balogun, 2016).

Some terms in accounting treasury, namely fraud auditing, forensic accounting, investigative accounting, litigation support, and valuation analysis ". In everyday use litigation support is the broadest term and covers the other four terms. Bologna and Lindquist did not touch the term valuation analysis (Olukowade & Balogun, 2016).

This analysis is related to accounting or accounting elements. The parties in dispute in business dealings can ask one party to buy all of the other party's shares, or they can agree that the final buyer is the bidder submitting the highest price. The case of corruption, a calculation is needed on how much this country is losing. This is a general description of the scope of forensic accounting in the private or business sector.

b. Practices in the Government Sector

In the public sector (government), the practice of forensic accountants is similar to what was described above, namely in the private sector. The difference is that the stages in the entire set of forensic accounting are divided among various institutions. Some institutions conduct audits of state finances, there are several institutions that are part of the internal government, there are court institutions, there are institutions that support activities against crime in general, and corruption in particular such as (PPATK), and other institutions such as the KPK. There are also non-governmental organizations that function as pressure groups.

Each of these institutions has a mandate and authority regulated in the constitution, laws or other provisions. This mandate and authority will colour the scope of forensic accounting applied. Besides, political conditions and various other conditions will affect the scope of forensic accounting applied, including legal or non-legal approaches. The impact that occurs in the government sector if there is fraud is the disruption of the implementation of state administration. If not supported by vigorous law enforcement, accounting standards and others, the level of corruption and weakness in the administration of the country will increase.

2.3 Fraud

Fraud is a deliberate fraud that can cause losses unnoticed by the injured party and provides benefits for the perpetrators of fraud (Reurink, n.d.). In everyday terms, fraud is given a different name, such as theft, seizure, extortion, exploitation, embezzlement, forgery, and others. Fraud generally occurs because there is pressure to misuse or encouragement to take advantage of opportunities that exist, and there is justification (generally accepted) for these actions. Misstatement consists of two types, namely, error and fraud (Richhariya, 2012). Fraud is translated as cheating per Statement of Auditing Standards (PSA) No. 70; likewise, the errors and irregularities are each translated as errors and irregularities per the previous PSA No. 32.

2.3.2 Causes of Fraud

The factors that cause fraud occur first because of the opportunity (opportunity), by knowing the perpetrators can see the opportunity to teach their fraud activities in order to get wealth and profit. Second, the pressure (pressure) where the financial or non-financial situation is the most usual incentive to commit fraud. Third, rationalization occurs because jealousy, resentment, anger, want to get rich quick and believe they are high can be a motivator for someone committing fraud. These factors are better known as the fraud triangle.
The cause of fraud explained by Bologna with GONE theory consists of four factors, i.e. (Reurink, n.d.):

1. Greed, associated with the existence of selfish behavior that potentially exists in every person.
2. Opportunity, relating to the state of an organization or community institution in such a way that there is an opportunity for someone to commit fraud against it.
3. Needs, related to the factors needed by individuals to support their lives which, according to him, is reasonable.
4. Exposure (disclosure), relating to actions or consequences that will be faced by perpetrators of fraud if the perpetrators are found committing fraud.

2.3.3 Signs of a Fraud

Fraud can be detected as early as possible if management or internal auditors are aware of these signs of fraud. Some of the signs of fraud are (Reurink, n.d.):
1. There are striking differences in the number of financial statements from previous years.
2. There is no clear division of tasks and responsibilities.
3. Someone handles almost all critical transactions.
4. Transactions that are not supported by adequate evidence.
5. Difficult company development.

2.3.4 Elements of Fraud

Elements of fraud or fraud are as follows (Imoniana, 2013):
1. A false agreement of material facts, or in some instances an opinion.
2. The desire to do something wrong or to achieve a goal that is not consistent with regulations or public policy.
3. Disguising a goal through forgery and misrepresentation to carry out a plan.
4. The offender's confidence in the victim's negligence or inaccuracy.
5. Concealment from evil

2.3.5 Fraud Classification

Fraud can be classified into three types, according to the Association of Certified Fraud Examinations (ACFE) viz (Popoola & Che-Ahmad, 2013):

a. Financial Statement Fraud committed by management, namely in the form of material misstatements of financial statements that are detrimental to investors and creditors. This fraud can be financial or non-financial.
b. Asset Misappropriation Asset misuse can be classified as 'cash fraud' and fraudulent inventories and other assets, and fraudulent, fraudulent expenses.
c. Corruption

Corruption occurs when it meets three criteria which are a condition that a person can be charged with a corruption law, the three conditions are: 1) against the law, 2) enriching oneself or another person or corporation, 3) harming the country's finances or the country's economy.

2.3.6 How to Prevent fraud

The root of the problem of fraud is "fraud by need, by greed, and by opportunity". The purpose of the phrase is if we want to prevent fraud, eliminate or suppress the cause as little as possible. An internal auditor can also do several things to prevent fraud, among others (Olukowade & Balogun, 2016) are:

1. Build an excellent internal control structure.
2. Active control, by way of performance reviews, information processing, physical control, segregation of duties.
3. Improve organizational culture through the implementation of the basic principles of Good Corporate Governance (GCG).
4. Making the internal audit function effective.

2.4 Fraud in a digital environment

Fraud in a digital environment is fraud related to computers or information technology (IT). The United States Department of Justice defines computer fraud as any illegal act that requires knowledge of computer technology to initiate fraud, investigate, or implement it. Computers have a significant influence on the environment of modern society and have resulted in many changes in a short period. Each company is also not immune from the use of information technology. The advantages of computers in the form of speed and accuracy in completing work to reduce the amount of labour, costs and minimize the possibility of making mistakes, resulting in people increasingly dependent on computers. Negative impacts can arise if an error occurs caused by computer equipment that will result in substantial losses for the user (users) or interested parties (Justenhoven et al., n.d.).

In today's world, information is the main asset and knowledge is power. Fraud in a digital environment is not a myth; several large and high cases occur due to the IT environment. The development of crime by using computer technology is increasingly diverse. To minimize fraud cases in a digital environment, the key lies in management to develop systems and procedures to prevent or increase the possibility of detection.

2.4.1 Fraud Related to Computers

Fraud in accounting is an act that causes reporting errors in financial statements. A crime related to a computer, in extensive terms, means a crime that has been committed or abetted through the use of a computer and a crime in which the computer itself is a victim.

Crimes commonly used with computers include embezzlement, property theft and proprietary information, fraud, impersonation and counterfeiting. A crime related to a computer is a crime related to work/position. That is, this is done by people who have the skills, knowledge and access. Fraud is easier for people in the organization than for outsiders. Therefore, it is essential to look at computer-related crime from various perspectives (Charlesworth & Charlesworth, 2019):

1. Individual crime and motivation.
2. External environmental factors that increase motivation to commit computer crime.
3. An internal organizational culture that minimizes or maximizes the possibility of fraud.

2.4.2 Reasons for Fraud in a Digital Environment

Several compelling reasons make the automated accounting system tend to open up opportunities for fraud. The principal reason is the possibility of the functioning of the computer without human involvement (impersonal). Fraud in the information technology environment usually occurs because of (Charlesworth & Charlesworth, 2019):

1. Controlling that is too old-fashioned and does not perform its barrier function adequately, at least for the average white-collar criminal.
2. Normal, rigid controls emphasized in a manual system suddenly disappear because of an automation system.
3. Management seems to be ready to face the challenges of securing the computer in its face.
4. Computer suppliers can be understood, more interested in selling innovative application solutions.
5. Employees who usually are overly enthusiastic about safeguarding physical assets are generally apathetic to EDP safeguards.
6. Auditors cannot follow the challenges of the presence of a modern system.
7. Access to the system has increased dramatically since the late 1970s.
8. System users are no longer intimidated or scared by automation.
9. Outsiders have a better chance of penetrating the network that results in fraudulent "encryption" dates sent through most networks and increases the use of "dial-up" connections.

2.4.3 Types of fraud in digital environments

Many cases of computer fraud that can not be revealed in the company environment because fraud perpetrators have used various methods to commit computer fraud. The categorization of computer fraud through the use of a data processing model can be detailed as follows(Charlesworth & Charlesworth, 2019):

i. The simplest and most common way to carry out fraud is to change computer input.
ii. Computer fraud can be done through the use of a system (processor) by unauthorized persons, including theft of time and computer services as well as the use of computers for purposes outside of the initial job description.
iii. Computer fraud can be achieved by disrupting software that processes company data or computer technology. This includes changing software, making illegal copies or using it without authorization.
iv. Computer fraud can be done by changing or destroying company data files or making copies, using or searching data without authorization.
v. Computer fraud can be carried out by stealing or misusing system output.

In general, computer fraud can be categorized as follows (Charlesworth & Charlesworth, 2019):
1. Data theft: such as programs, list of letters, confidential records.
2. Theft of equipment: such as hardware or software.
3. Service theft: the use of computer resources without being authorized.
4. Property crime: computer usage
5. It is not legal to transfer property.
6. Financial fraud: the use of computers for financial processing, theft, or diversion of funds.
7. Sabotage: physical assault on facilities
8. computer or components to make the system inoperable.

2.4.4 Fraud Prevention in the Digital Environment

Several ways can be done to prevent fraud, one of which is that a company makes specific standards that can significantly reduce the potential for fraud and the losses it can produce. These standards are making fraud less common, increasing the difficulty of committing fraud, improving detection methods, reducing losses due to fraud, prosecuting and imprisoning perpetrators of fraud.

Another way that can be done to prevent computer fraud is to design a system that is equipped with sufficient internal control so that computer fraud is difficult to do by outsiders or people in the company. Ways of protection that can be done by organizations/companies to prevent the emergence of computer fraud, i.e. (Charlesworth & Charlesworth, 2019):

1. Personnel screening
2. Job defined
3. Segregation of duties
4. Professional ethics
5. License
6. System design control
7. Physical access security
8. Electronics access security
9. Internal control and edit

Current technology is protecting the flow of communication in an organization.
Although this security technology is not based on the mindset of detecting and preventing fraud, if used appropriately, this solution can provide reports on the possibility of an instant fraud attempt. The solution to prevent the possibility of fraud viz (Charlesworth & Charlesworth, 2019):

1. Firewalls are an effective security device that filters or blocks the traffic that passes through it.
2. Messaging (E-mail): notifying employees that they should have no expectation of privacy in connection with e-mail or other uses of company networks and computer systems can act as an excellent deterrent to fraud activities.
3. Messaging (Instant Messaging): The most popular IM services are AOL, Yahoo, MSN, and ICQ. Most users have this false assumption that their employees cannot log this traffic. The solution to identify this IM traffic from other web traffic using the same TCP port. When traffic is identified, it can be blocked or controlled by specific IP addresses or users who have access to IM.
4. Content Filtering: Content filtering solutions are mainly used to restrict or log access to certain websites on the internet.

Computer fraud must be prevented before it happens, is the responsibility of management to create a conducive environment so that it can prevent computer fraud.

2.5 Conceptual Framework

The rapid development of technology can spark new ideas for fraud perpetrators to commit fraud through the technological environment, which is often referred to as fraud in the Digital Environment. Both accounting students and auditors need to be familiar with the role of IT and play in the digital environment. The business has also grown in the use of technology and reliance on computer-based systems. The conceptual framework, as follows:

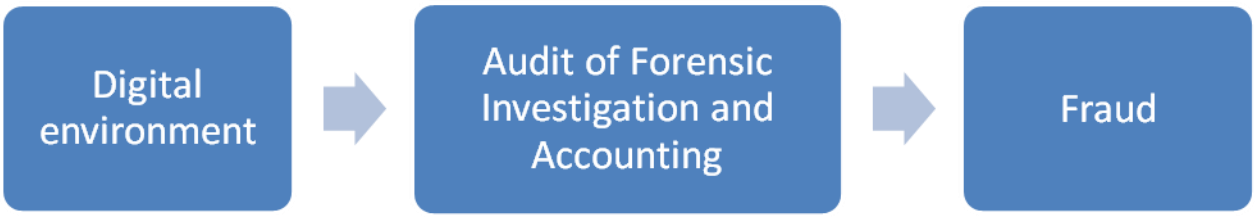

Figure1. Conceptual Framework

Research Methods

Researchers conducted a library study by collecting several economic journals and books relating to the problem under study. The data collection method in this research is done by interpreting and analyzing qualitative data, and this is the most challenging task in conducting a case study. This data collection is also done manually by searching for data through librarian references. The data taken are theories regarding forensic accounting, investigative audits and fraud related to the digital environment.

Research Results And Discussion

Forensic accounting arises because of the rapid development of fraud. To prove the indication of fraud in a digital environment, the auditor can do computer forensics. In the end, to solve a fraud in a digital environment effectively, need to test the system as a detective not as a user. This is the task of a forensic accountant to uphold the law and secure evidence, reconstruct the crime, and ensure that the evidence collected is useful at trial.

1. Forensic Accounting and Audit Investigation of fraud in the Digital environment

The science of forensic accounting arises because the development of fraud is increasingly rapid. Forensic accounting is the use of expertise in the field of auditing and accounting combined with the ability to investigate to solve a problem or financial dispute or suspected fraud which will ultimately be decided by a court/arbitration / other case settlement.

The number of fraud cases contained in the digital environment, then the cases are analyzed in more detail by doing computer forensics. Computer Forensics is the application of analytical and investigative techniques to identify, collect, examine and protect evidence or digital information. The main steps that must be taken in computer forensics are:

i. Imaging
A device is connected to one communication port (parallel port), and this tool will record all the data that is on the electronic storage media (hard disk) in the computer entirely, no more or less. Imaging is crucial because these steps are only done on the results of imaging and not on the original data. Hard disks are sometimes often separated from the computer housing, copied in full byte by byte without being added or subtracted.

ii. Processing
After getting a mirror image from the original data, the image must be processed to recover files that have already been deleted or rewritten with the current file. By restoring copied images, files, and folders will appear like the original data storage media.

iii. Analyzing
The final step, the investigator shows his expertise, creativity, and application of original ideas. Fraudsters and criminals generally save their files in my documents or my pictures folder.
In investigating fraud in a digital environment, a forensic accountant must be able to develop a case theory that is suspected of fraud and then incorporate it into the scientific method. Forensic accountants must also recognize digital evidence that is potential evidence and evidence for evidence in court. The scientific method in question includes identifying problems (hypotheses), gathering evidence and data, analyzing data to test hypotheses, and drawing conclusions.

2. Forensic Purposes in a Digital Environment

The purpose of Computer forensics is to secure and analyze digital evidence. From data obtained through surveys by the FBI and The Computer Security Institute, in 1999, said that 51% of respondents admitted that they had suffered losses primarily in the financial sector due to computer crime. The purpose of computer forensics is to describe the present state of a digital artefact. Digital artefacts include a computer system, storage media (such as a flash disk, hard disk, or CD-ROM), an electronic document (e-mail, or JPEG image), or even a series of packets that move on a computer network. Forensic computers are used to eradicate corruption, fraud in the internet world.

3. Forensic Terminology

1. Digital evidence (digital evidence): information obtained in digital form or format, for example, e-mail.
2. Four key forensic elements in information technology:

a. Identification of digital evidence.
   At this stage, identification is carried out where the evidence is, where the evidence is stored and how it is stored to facilitate the next stage.
b. Digital evidence storage.
   Digital evidence can be lost because of poor storage, including the most critical stages in forensics.
c. Digital evidence analysis.
   Retrieval, processing and interpretation of digital evidence is an essential part of the analysis of digital evidence.
d. Presentation of digital evidence.
   The trial process, in which digital evidence, will be tested by existing cases. The presentation here is in the form of digital evidence relating to the case being tried.

4.Information Technology Case Investigation

Some things that need to be done and explained by investigators, namely:
a. Make copies of entire log data, files, and others deemed necessary on a separate media.
b. Make fingerprints from data mathematically, for example, hashing algorithm, MD5.
c. Make fingerprints from copies mathematically.
d. Make a master list hashes.
e. Proper documentation of everything that has been done.
Evidence used in detecting fraud in the IT environment is:
a. Hard disk.
b. Logs
c. Stand-alone system
d. Floopy Disk or other media that is removable.
e. Network system.
Besides, it is necessary to carry out further investigations where the methodology mentioned earlier is used. Of the two methods, search, and seizure methods are more widely used than information retrieval. Although on the other hand, it does not hurt if the search and seizure method is equipped with searching for more detailed information. The stages in the search and seizure method are:
1. Identification and research problems
In this case, identification is the identification of the problem being faced, whether it requires a fast response or not. If not, then continue in-depth problem research.
2. Make a hypothesis
Making a hypothesis after going through the process of identifying and researching problems that arise, so that the data obtained during the two processes above are produced hypotheses.
3. Test hypotheses conceptually and empirically
The hypothesis is tested conceptually and empirically whether the hypothesis can already be used as a conclusion or not.
4. Evaluate the hypothesis based on the results of testing and retesting if the hypothesis is far from what is expected. Evaluate hypotheses for other impacts if they are acceptable.

4. The role of computers in fraudulent activity

Computers and digital media are increasingly being used in activities against the law. Computers can also be tools or means of crime such as the use of cellular phones to extort, information stolen from digital media, or as a means of storing information about the crime. The rapid development of fraud in information technology requires that forensic accountants recognize digital evidence which is potential evidence and evidence for evidence in court. Fraudsters use computers to smuggle information in terms of stealing hardware and software. Computer systems are also used to create a fake or real identity (passwords) that are stolen, downloading from information stored in the system or database, and others. Computers are also used to store data, such as names, addresses, details of contracts made with suppliers who give "kickbacks" or kickbacks.

Fraudsters such as computer hackers, they attack systems and databases of credit card issuers to steal information about customer credit cards. Hackers also store stolen information on computers or digital media. From the explanation above, it can be seen that the role of computers in conducting fraud is huge. Using a computer can make it easier for fraudsters to get the information they need to commit a planned crime.

Conclusion

This study found out from the extant literature of the previous piecemeal studies that the impact of skills and mindset on fraud risk assessment (forensic accountant and auditor) in the digital environment cannot be overlooked. Thus, there is a need for a holistic approach to examining the impact of skills and mindset (forensic accountant and auditor) on fraud assessment task performance in the digital environment. Any holistic study which is intended to reduce fraud and other fraud-related crimes would be much desired, timely, and relevant, especially in Indonesia's digital environment.

References

Beneish, M. D., Bressler, L., Clements, L. H., Knudstrup, M., Jones, K. L., Krishnan, G. V, Spathis, C. T. (2011). The role ole of forensic a accountants in fraud investigations: Importance of attorney and judge's perceptions. Contemporary Accounting Research, 3(2), 417–439. https://doi.org/10.1108/0268690021042432

Charlesworth, A., & Charlesworth, A. (2019). The digital environment. Digital Marketing, 23(4), 3–13. https://doi.org/10.4324/9781315175737-1

Imoniana, J. O. (2013). Forensic accounting and corporate fraud. Journal of Information Systems and Technology Management, 10(1), 119–144. https://doi.org/10.4301/s1807-17752013000100007

Justenhoven, P., Sechser, J., & Loitz, D. R. (n.d.). Digital Audits of Financial Statements. Retrieved from www.pwc.de

News, A. C. (2017). Impact of digitization on the audit profession. 33–35. Retrieved from https://assets.kpmg.com/content/dam/kpmg/ch/pdf/ac-news-8-impact-digitization-en.pdf

Olukowade, E., & Balogun, E. (2016). The relevance of Forensic Accounting in the Detection and Prevention of Fraud in Nigeria. International Journal of Accounting Research, 2(7), 67–77. https://doi.org/10.12816/0017351

Popoola, O., & Che-Ahmad, A. (2013). Forensic accounting knowledge and skills on task performance of fraud risk assessment: Nigerian public sector experience. The Global Symposium on Social Sciences (IBSSS) 2013 Okinawa, Japan, (66676). Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2654724

Rapp, H. P. (2010). Auditing the. Financial Executive, 23(4), 62–63.

Reurink, A. (n.d.). Financial Fraud A Literature Review Arjan Reurink MPIfG Discussion Paper.

Richhariya, P. (2012). A Survey on Financial Fraud Detection Methodologies. 45(22), 15–22.

Scotland, A. (2017). Digital Audit Strategy, 2017. (October).