Employee fraud and misconduct: empirical evidence from a telecommunication company

Anuar Nawawi
Faculty of Accountancy, Universiti Teknologi MARA, Shah Alam, Malaysia, and
Ahmad Saiful Azlin Puteh Salin
Faculty of Accountancy, Universiti Teknologi MARA Perak Branch Tapah Campus, Tapah Road, Malaysia

Received 14 July 2017
Revised 18 September 2017
27 October 2017
Accepted 31 October 2017

Abstract

Purpose – The purpose of this study is to examine whether policies and procedures, one of the fundamental elements in the internal control environment, are adequate and effective in preventing fraud and unethical practices committed by employees of a company. In addition, this study attempts to assess the awareness and understanding of employees on the existence of relevant company policies and standard operating procedures for internal fraud and misconduct deterrence.

Design/methodology/approach – Five cases from one Malaysian telecommunication company were randomly selected as a case study. Content analyses were conducted on actual cases of internal fraud and wrongdoings that were investigated and the enforcement that was discharged by the company.

Findings – This study found that the company has sufficient policies and standard operating procedures to curb internal fraud and wrongdoing. However, they are ineffective and malfunction when responsible personnel violate or override the policies and procedures, irrespective of whether this is caused by carelessness, poor knowledge or clear intention to act dishonestly.

Research limitations implications – This study was conducted on only one company with a limited number of investigated fraud cases. Access to higher number of fraud cases, particularly those that involved large amount of losses and considered as high-profile cases, were denied because of confidentiality.

Practical implications – The study found that weak compliance to internal controls provides opportunities for fraud to occur, consistent with the fraud triangle theory. Fraud, committed both outside and inside an organization, can be considered as a worrying problem in the organization because of its severe impact on the reputation and bottom line figures of the company. The study provides important information to management to strengthen their compliance with the internal control system generally and policies and procedures particularly.

Originality/value – This study is original, as it focuses on the actual fraud cases that occur in the telecommunication industry, which is under-researched in fraud literature, particularly in developing markets such as Malaysia. Prior empirical research on fraud and unethical practices has concentrated on factors that contribute to fraud and the financial and non-financial impacts of fraud in an organization.

Keywords Misconduct, Internal control, Telecommunications industry, Policy, Procedures, Fraud

Paper type Research paper

Introduction

The telecommunications industry is constantly undergoing transformation and is headed for convergence. A combination of various products and services is offered such as smart phones, fixed and broadband services, service delivery platforms and social networking. As a result, the demand for products and services has increased. Technology continues to innovate; thus, change is unavoidable, while risks also arise.

Information and Computer Security
Vol. 26 No. 1, 2018
pp. 129-144

2056-4961
DOI 10.1108/ICS-07-2017-0046

Therefore, it is important for the telecommunication company to state the principles and set the tone by which business is to be conducted based on policies of risk and internal controls. These policies are designed to continuously identify, assess, monitor and mitigate risks, especially fraud and wrongdoing, among their employees, contractors, vendors, suppliers, dealers and business partners.

Documented policies and procedures need to be in place for all major aspects of any company's business. It is a most fundamental aspect and a foundation for strong internal controls. It should be regularly reviewed and updated to ensure all the documents remain effective and continue to support the organization's business activities. For example, a job manual serves as a guideline for employees, contractors, vendors, suppliers, dealers and business partners to carry out their routine jobs in the workplace and facilitate business conduct when dealing with external parties and assist to deal with key issues, such as bribery, conflicts of interest, insider trading and data integrity. Hence, policies and standard operating procedures (SOPs) are essential for a company to prevent or minimize losses from fraud and protect the company from misuse by those with criminal intent. It is also a valuable tool to help prevent mistakes because of poor judgment.

Even so, the cases toward internal fraud and wrongdoings among employees and top management were highly reported every year, including Malaysia. This is possibly because of poor corporate governance practices (Nor *et al.*, 2017; Ahmad *et al.*, 2016; Hashim *et al.*, 2014; Jaafar *et al.*, 2014; Husnin *et al.*, 2013; Hamid *et al.*, 2011) and inadequate internal controls, which cause fraud and misappropriation to fail to be detected and prevented (KPMG, 2009). Puah *et al.* (2009), for example, found that poor cash security exercises, insufficient staff supervision and dysfunction of internal auditing to efficiently and effectively operate lead to the malpractice, fraud and mismanagement. This indicates adverse consequences if a company only establishes an inferior level of internal control practices. A survey by KPMG Malaysia to the chief executives of public listed companies on the Malaysia Bourse also confirmed that a majority of respondents believe the policies, procedures and controls are not adequate to prevent fraud (KPMG, 2013). In contrast, high-quality audit such as using large audit firms as an external auditor likely to reduce financial statement fraud (Husnin *et al.*, 2016; Lisic *et al.*, 2014; Asmuni *et al.*, 2015).

Based on this phenomenon, this study intends to first determine whether a company's policies and SOPs are successful in preventing fraud and, second, to assess the level of awareness and understanding among employees on the existence of relevant company policies and SOPs on internal fraud prevention. In general, this study will attempt to answer the following research question:

RQ1. Can policies and procedures prevent employee fraud in a company?

This study contributes in several ways. First, it will produce an important component of establishing specific policies and SOPs to the managers of the company. The policies should not be merely established just for formality and audits' sake. It must be proven workable and accessible by any members of the organization. Therefore, it is crucial to ensure that the employee can easily access and obtain such documents.

Seconds, findings from this study might be useful to help clarify the reasons as to why organizations generally and telecommunication companies particularly require sets of policies and procedures to guide their operations and enable them to measure how effective these policies and procedures are, as this industry continues to grow and become profitable.

Third, this paper will demonstrate that internal fraud, including employee misconduct and wrongdoings, might be reduced if documented policies and SOPs are in place for all major aspects of a company's business and are understood by employees and regularly

reviewed and updated to ensure that they remain relevant and effective. The results of this study will share the advantage of establishing and maintaining a set of company policy and SOPs as a reference document to set limits, maintain control and resolve disputes among employees and other interested parties.

Finally, these findings will advance theoretical understandings and add to the body of the literature on the importance of policies and procedures in combating fraud and unethical practices, information of which is scarce in literature, particularly from developing countries like Malaysia. Much prior empirical research on fraud and practices concentrates on the factors that contribute to fraud and the financial and non-financial impacts of fraud on the organizations.

This paper is organized as follows. The literature review is followed by research methodology. Section 4 describes the findings, while Section 5 contains the discussion. Section 6 contains the conclusion and implications of the study. The last section describes limitations and suggestions for future research.

Literature review

Overview of fraud

Vona (2012) suggests that fraud is an act committed on an organization by the organization or for the organization. It uses trickery and deception to gain advantages, commonly a financial advantage on another person or organization (ActionFraud). The acts are committed either individually or by groups (Free and Murphy, 2014), by an internal or external source, and normally with intentional and concealed elements. The acts are typically illegal or denote wrongdoing, such as in cases of manipulation of financial statement, policy violation and ethical misconduct.

ACFE (2010) describes three types of fraud against organizations. First is asset misappropriation, which is any scheme that involves the theft and misuse of an organization's assets, corruption and fraudulent statements. Second is internal fraud or fraud against organizations; third, wrongdoings impose enormous costs on a company. Based on a study carried out by ACFE (2010), this type of fraud can be difficult to detect; normally, such illegal and unethical practices are detected by a tip, internal audits and external audits and also by internal control activities executed by a given department.

Fraud mostly causes a loss of company funds. The real direct costs of economic crimes to an organization can be difficult to calculate because many companies do not report fraud, worrying about poor perceptions of stakeholders and tarnishing the reputation of the company. Paine (1994) explained that, usually, executives are quick to describe any wrongdoing as an isolated incident and assume that the company could bear the responsibility for an individual's misdeeds. In fact, unethical business practices such as wrongdoings basically reflect the values, attitudes, beliefs, language and behavioral patterns that define an organization's operating culture. Furthermore, the total detected losses are only one-third, while the remaining two-thirds remain invisible and untraceable (KPMG, 2010).

For example, occupational fraud and abuse costs the companies worldwide, typically exceeding US$3.5 trillion a year (ACFE, 2012). China has lost more than US$2.8bn annually since the 2000s because of fraud (Zhou, 2006) and billions of dollars because of bank fraud (Cheng and Ma, 2009). In Malaysia, a survey conducted by PriceWaterhouseCoopers (PWC) found that 7 per cent of respondents claimed that they lose between US$5mn to US$100mn, while 37 per cent of respondents estimated that they lose between US$100,000 to US$5mn (PWC, 2011). This is concurrent with a prior KPMG survey, which reported that a significant number of respondents believe that fraud is a major problem for businesses

operating in Malaysia. In addition, a majority of respondents (61 per cent) without hesitation forecast that levels of fraud will increase in the future (KPMG, 2009).

Unfortunately, financial losses are not the only consequences of economic crime because other nonfinancial losses also have a significant impact on the company. Damage to employee morale, brand impairment, tarnished company reputation, deteriorated business relationships and loss of consumer confidence weaken public trust and ruin market share value, which may cause a company to collapse in the long run. Worse yet, fraud and unethical practices not only have an impact on a single entity such as poor performance of a company (Salin *et al.*, 2017; Khadijah *et al.*, 2015) but can spread to others and on a large scale – and possibly shake the country as a whole (PWC, 2011). The Greek economic crisis is a good example. This combination of various fraud, scandals, mismanagement, corruption and other malpractices almost ruined not only Greece but also paralyzed the European Union's financial system.

Policies and procedures in the internal control systems

Under the Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework, standards and process are located under the control environment components. They include the most fundamental and important elements that need to be established because they provide a basis for internal control implementations across organizations, at all levels (top, middle and lower) both vertically and horizontally (COSO, 2013). It helps to facilitate effective and efficient operations, ensure the quality of internal and external reporting and compliance with applicable laws and regulations (Financial Reporting Council, 2005). Well-designed policies and procedures ensure a company's objective is successfully achieved (Securities Commission, 2007). In addition, it helps companies take corrective action when something goes wrong, assists in training new staff, helps reduce and prevent errors and facilitates the workforce in understanding business management and operations (CPA Australia, 2008).

The important issue regarding policies and procedures in the internal control systems is compliance. Policies and procedures are meaningless if constantly violated and overridden by personnel. Some may argue that internal control is unnecessary, a waste of time or "red tape" (CPA Australia, 2008). Because of this, the tone at the top, from the highest authority in the organization, is important to show a good example of conformance to internal control procedures. This example, then, will be replicated from lower-level management to the lowest layers of the organization. The KPMG survey shows that personnel who override internal controls may be doing so for their own benefit and may be attempting to defraud a business (CPA Australia, 2008). In contrast, morally and ethically behaved employees will have a favorable impact on their organization (Manan *et al.*, 2013).

Without decent standards and processes, other components of COSO framework such as risk assessment, control activities, information and communication and monitoring activities will be paralyzed. Prior research has shown that a firm with a small size, newly established, weak financial performance, has complex and complicated business transactions, growth at exponential rate and under business transformation such as restructuring, has weaker internal control (Doyle *et al.*, 2007). This weakness will lead to a higher cost of capital (Ogneva *et al.*, 2007), many errors in financial and nonfinancial data (Rahim *et al.*, 2017) and in case of not-for-profit organizations, this entity will face trouble in obtaining support from the government and contributors to fund their operations.

Fraud triangle theory

Fraud in organizations can be explained by using a fraud triangle theory (Cressey, 1973). This theory suggests that pressure, opportunities and rationalizations needed before fraud can occur. Pressure usually comes in two forms: personal and company. Personal pressure is normally associated with financial pressure, although nonmonetary achievement can be the other perpetrator motivation (Dilla *et al.*, 2013). An individual feels worried if he is unable to maintain a required lifestyle with a limited income. Company pressure is more complicated. This is a burden that needs to be borne by company managers, especially if the expectations of the top management, for example, board of directors and shareholders, are high. Manipulating financial statements to show favorable results is an example of fraud committed by this kind of person.

Opportunity is the chance to commit fraud. It is linked to poor control environment that increases the ability of the fraudster to conceal the fraud evidence while at the same time reduces the possibility of the fraudster to get caught. Lack of job rotation, coupled with over-reliance on one person to conduct a job, lays open the opportunity for that person to perpetrate fraud.

Rationalization is an excuse to claim that fraudulent actions are just and right. It can be done in a few ways. First is referring to other people performing the same deeds but with no action taken. Second is cultivating a sense of unfairness treatment by the organization, such as underpaid employment, no promotions and lack of employee benefits like in other companies. Bhattacharya and Marshall (2012) suggest that rationalization is the main motive of the top-level white-collar crime of insider trading in the USA.

Research method

Five fraud cases from one telecommunication company were selected to be examined in this study. The case study approach was used because, based on Smith (2015) and Bromley (1986), a case study is the best method to use if actual setting of the research can be examined and real-world contexts can be obtained. Miller and Brewer (2003) also posit that the case study method provides interesting and inspiring research in social science because it offers in-depth and detailed understanding about the problems and issues under research, while Leedy and Ormrod (2005) suggest that this approach is appropriate to learn and to examine little-known and poorly understood environments, which are generally difficult to access via normal research process and are not publicly available. This has allowed the researchers to investigate the chosen company or case in depth with meticulous attention given to details (Zikmund *et al.*, 2012).

Based on these arguments, case study is the most appropriate method of research, as the permission was granted to scrutinize a few actual fraud cases that occurred in this company. These fraud cases provide an opportunity for rich analysis of the situation and are likely to have practical implications that are beneficial to practitioners. Besides, the opportunity arises to examine the actual practice in response to the event that provides potentially unique findings. The case documents are highly sensitive and not publicly available. Because of this, specific and identical information such as organization profile, name and background of the fraudster and date and time of the fraud cannot be revealed in this paper. Prior study on fraud and malpractices also used a similar approach (Rahim *et al.*, 2017; Omar *et al.*, 2016; Zakaria *et al.*, 2016).

The sample of the case study consists of internal fraud cases and wrongdoings committed by employees. All cases were reported from January 2012 until September 2013 by various parties and have the possibility to harm the company. A total of 152 cases were closed from January 2012 until September 2013, and 299 enforcement cases were completed

during that period. The total number of cases for the investigation and enforcement activities for this company from January 2012 to September 2013 is tabulated in Table I.

This study uses content analysis on various company documents and archives for data collection. Cross-checking the data via multiple documents was conducted to enhance the validity of the research (Hodson, 1999). The cases selected in this study are based on actual cases that were investigated and enforcement, which was discharged. Name of employee involved is not disclosed because of confidential information. The case files were obtained from the fraud prevention and investigation department, while the company policy and SOPs were retrieved from the document control system via the company intranet.

Findings

Five cases involving fraud and misconduct at the company from January 2012 to September 2013 were selected and analyzed. The cases selected in this study are based on actual cases that were closed and analyzed based on various policies and SOPs to measure their effectiveness in curbing fraud. All the data collected from the cases have been analyzed in three distinct phases as recommended by Malhotra (2010), namely, data reduction, data display and data conclusion. In the data reduction phase, information that is emphasized and the most important was selected, whereas non-important information was eliminated. At the same time, the common theme was established. In the second phase, data display, visuals and diagrams were used to observe if there is any pattern, relationship or trend among the information selected or the theme. Last phase is the data conclusion. In this step, the meaning of the theme or information is analyzed and verified.

Case 1: loss of company laptop

On a particular date, the risk management department received a report on the loss of a company laptop. The incident happened at approximately 10:30 p.m. The responsible staff claimed that, on the day of the incident at around 8:15 p.m., the employee parked her car in front of a restaurant. Because of heavy rain, she decided to leave her laptop inside the car. She was rushed from her office to the place for a meeting and arrived at the location around 8:15 p.m. She kept her laptop in her black personal bag and placed it under the driver's seat. After she locked her car using the alarm system, she went to a nearby restaurant for a meeting. She returned to her car around 10:30 p.m. and found the passenger window behind the driver's window broken. After thorough checking, she realized the company's laptop was missing. The employee went to the nearest police station and lodged a police report.

Findings from Case 1

This study found that the employee member was negligent in keeping possession of the company's laptop, as she failed to keep the portable computer with her at all times or deposit it in a secure location, for example, in the office (in a locked closet or safe). This caused the laptop to become lost because of theft. Total losses because of staff negligence amounted to RM 2,432.

Table I.
Total investigation and enforcement activity

Activity	Jan 2012-Dec 2012	Jan 2013-Sept 2013
Investigation	79 cases	73 cases
Enforcement	174 cases	125 cases

During the investigation, the employee claimed that she was not aware of the company policy. The significant relevant policy related with this case is the company's access control standard policy. The clause states that:

> Mobile equipment such as notebook and smartphone must be properly secured by the user at their workplace and not left unattended. Staff possessing a portable, laptop, notebook, handheld, or other transportable device containing confidential information must not leave these items unattended at any time.

Case 2: loss of demonstration unit (iPhone)

The service quality management department encountered a case of the loss of demonstration unit (iPhone 4S) when it had completed its outlet stock audit and review for fourth quarter at marketing department. The police report lodged by the employee indicated that the incident happened a few months ago around 2:00 p.m. at her workstation. The employee stated in the report that she had reported the incident to the company and did request for CCTV recording to view the possibilities that the device was taken out. However, the surveillance system was unable to capture the possibilities, as her workstation is not within the CCTV coverage area. As a result, there was no sign to show the occurrence of theft at her workstation, which possibly caused the absence of the parcel or demonstration unit.

On the day of the accident, the human resource administration staff had handed over six parcels to her that contained all returned demonstration units from outlets nationwide. All parcels were on her desk before properly securing them in a store cabinet. The employee discovered that a parcel went missing from her desk when she came back to her work station after leaving it for about half an hour.

The employee claimed that there was no specific process and procedure for demonstration unit receipts and return handling. Basically, the transactions are based on trust. The employee affirmed that the accident might have happened because there was an opportunity for a stranger or outsider to take the parcel on her table because of her open and accessible workstation. In addition, the employee ascertained that she did notify her immediate superior regarding the incident and did follow-up. However, all was done verbally and gained no feedback. Her immediate supervisor confirmed that the employee did inform her regarding the incident, and the case was also acknowledged by higher authorities for their next course of action.

Findings from Case 2

The study found that the employee adhered to the procedure for handling lost stock, as she immediately notified her superior regarding the incident. However, the employee only filled out the lost incident report (LIR) six months after the incident occurred and lodged a police report. She rationalized her action not to immediately report the accident, as she was not aware of the related policy. Even though the employee claimed that she knew about the company policy and procedure shown to her, she did not realize that was also applicable to headquarter staff, especially for those handling demonstration units.

In spite of this, said staff was also not aware of particular requirements in regards to code of conduct and failed to take all reasonable precautions to safeguard the inventory or company asset, including to ensure the device be properly stored and kept secured against the risk of damage, pilferage and loss. The clause states:

> Employees shall be personally responsible for protecting the company's assets entrusted to them. Employees must take all necessary steps to prevent theft, loss, damage to, or misuse of assets belonging to the company, the occurrence of which must be reported immediately to the immediate superior.

The employee argued that although she had taken all the necessary steps to prevent pilferage and theft, adequate security measures should be taken, for example, restricted access to her workstation to minimize the risk of similar incident. Nevertheless, as stated in the company policies and procedures, the employee, as a custodian of the device, failed to notify or lodge an immediate report to the respective party regarding the incident. In addition, based on investigation, it was revealed that there is an element of negligence by the employee because she was careless and failed to take reasonable care to ensure proper custody of the demonstration unit when she left the device unattended for half an hour on her desk.

Case 3: unauthorized disclosure of customer information

The company received a complaint from a consumer claiming that someone requested his telephone bill statement without his consent or knowledge. Thus, the complainant required to know the person who had illegally printed out the document. He stated that four months of statements were found outside his house on a particular date. The complainant also asserted that he did not make any request to reprint his bill statement and alleged that somebody may have done it without informing him or getting his permission.

An email was sent to the senior technical manager at IT, billing applications management, requesting his assistance to provide an audit trail report for the complainant's mobile number with regards to the possibility of information disclosure of the customer information to a third party. The IT analyst through an audit trail report specified that one staff had reviewed the complainant's account. The responsible employee was an outlet executive at one of the branches and was responsible for the sales and service of the products, cash register transactions, assisting customers when they are facing problems and offering solutions or recommending services provided to the customer. In short, based on her job description, the employee had the capability to access customer information.

The employee rationalized her action of viewing the customer's bill by claiming that the bill was enquired by the customer. In addition, she needed to open the previous bill as the customer requested to track the consistency of call usage and charges. However, the employee failed to recognize or remember any interaction between herself and the customer who request the bill reprint and the complainant.

Based on the audit trail, it was discovered that the employee accessed the system, which indicated that said staff accessed the account belonging to the claimant. This action took place over nearly 5 minutes. It was confirmed by the IT network support lead that both Internet Protocol addresses belonged to the branch where she worked. Additionally, the surveillance system recording showed that the employee did handle one customer, who appeared to be a lady. The copy of the CCTV recording also illustrated that the employee did hand over some documents that looked like a reprinted bill.

The employee confessed that she was the one who passed the reprint bill statement to the third party without proper verification of the bill requestor such as an identity card or request letter of authorization for third-party request. Hence, she agreed that her action to reprint the bill statement without customer authorization was wrong, irresponsible and a violation of her duty as an outlet executive. The employee also noted that she failed to treat such information as confidential or take all necessary safeguards to protect this information. Her reckless action toward this case was because of non-compliance to policy.

Findings from Case 3

This study found that the employee knew about the policy and code of conduct, but she was not aware of and had never read the reprint of bill statement procedure. Based on all the

information and evidence gathered, it is confirmed that the outlet executive, who is a contract employee, failed to perform proper verification, that is, verify customer identity card or request letter of authorization for third party before proceeding with activities such as access the customer's account, viewed four months' bills of the customer's mobile number, reprint the bill statement and give the bill statement documents to a third party.

The employee also did not comply with the code of conduct because she failed to protect the company's proprietary information as stated:

> Proprietary Information – all information (whether in written or oral form and whether on paper or electronic form) relating to [. . .] customer information, databases, records and any non-published financial or other data that is not public information [. . .] It is critical that employees treat such information as confidential and take all necessary safeguards to protect this information.

Case 4: unauthorized collection of bill for payment

The company received an anonymous complaint via email that the customer had received a short message (SMS) from a mobile number offering the customer to settle the outstanding bill by half. This offer was illegitimate for the company's usual business transactions. Thus, the complainant requested that the company do further investigation pertaining to this offer.

An investigation revealed that one staff was detected performing the unauthorized transaction. These includes 98 cash payment transactions amounting to RM 94,928, which were updated using the user ID of the responsible staff. In that period, 47 accounts were affected by that activity and from that information, the investigation officer (IO) managed to identify the details (name and IC No.) of 31 customers.

As a customer service representative at the escalation department, she is responsible for handling cases of payment within a time frame, change of credit limit, conduct processes to cater to requests for delaying a full settlement of overdue or exceeded credit limit amounts to a later promise date and authorizing reconnection to reactivate accounts.

She stated that she knows how to use the system well. The employee rationalized her action to perform the transaction and claimed that, as an employee, she should use all the facilities provided by the company. She thus performed adjustments and payment transactions for her close relatives and family. At the same time, she also facilitated the customers who requested to make payments via phone call.

Findings from Case 4

This study found that the employee was aware of the code of conduct but never read and understood the contents:

> Employee conduct relates to the conduct of employees both on and off the job, where such conduct must not adversely affect [. . .] legitimate business interests of the company.

> Employees must consider the interest of the company when making decisions that will impact the company and not based on personal gains/favors, utilize the company's assets for business purposes only and not for personal gains [. . .]

In relating the access control standard policy, nevertheless, she understood and agreed with these following policies and clauses when they were shown to her.

> Password management: Password must be allocated during the creation of the user ID. The security and maintenance of the password is the responsibility of the user.

Sharing ID: Every user is prohibited from sharing their accounts, user ID and passwords unless special approval is obtained, document.

Case 5: unauthorized installation of 3G service

An individual came to the branch and claimed that he never requested the installation of 3G service and was now requesting a rebate. Further checking by the IO found that there were a few transactions that had been performed by another party without authorization. From the employment history, the complainant is the company's ex staff and tendered his resignation on 15 August 20XX. Based on the date of the transactions, IO detected the user who accessed the account on the days of the incident. Based on the Internet Protocol address, the workstation location belonged to the complainant. It was found that the unique ID belonging to the complainant was still active.

The investigation with the ex-supervisor of the complainant found that he received the resignation letter from the complainant on 15 August 20XX and had handed over the document to his team manager. Furthermore, the employee stated that his next action after the employee resignation was to complete a form for ID termination. However, because of workload, he failed to comply with the procedure. The employee agreed and was made aware of the access management policy.

Findings from Case 5

The study found that the installed 3G service was done performed by the complainant using his own ID, and the illegal misconduct and wrongdoing was performed at his workstation on 26 and 27 September 20XX before his resignation. Thus, no rebate was given for the complainant's account number. However, there is evidence to conclude that his supervisor failed to better manage the IDs granted to their subordinates. This is not in accordance with the user access management policy further explained below:

> Each unique User ID must not be reused after a staff or Vendor terminates their association with the company.
>
> Users must complete the User ID Request Form and approved by Head of Department. Once approved, IT Helpdesk shall assign the relevant request to Profile Admin Unit. This applies to all types of requests such as new ID creation, termination suspension, reactivation, password reset and profile amendments.
>
> People and Performance Division (also applicable to VADS HR) must inform Profile Admin Unit through official memo confirmation that the employee is ceasing employment to terminate the ID.

Discussion

Based on the content analysis of the file and document search of all the above cases, it is suggested that the company has sufficient specific policies and SOPs to curb internal fraud and wrongdoings. In fact, this study found that the documented policies and procedures are regularly reviewed and updated to ensure that they remain relevant, effective and continue to support the organization's business activities at all times as the organization continues to grow.

Almost all policies and procedures are supported by clearly defined and delegated authorities for its operating and capital expenditures, business plan and budget and procurement of goods and services. Additionally, certain policies and procedures, such as the Code of Conduct, were designed to ensure that all employees conduct their businesses

within the framework of applicable laws and regulations, as well as the company's policies and procedures.

The study found that the company in this case has total of 86 company policies divided into three categories: divisional policy, corporate policy and operational policy. A total of 807 SOPs have been established. The detailed numbers of company policies and SOPs are shown in Table II.

In addition, the study discovered that a complete manual was created to serve as a guideline for employee conduct in the workplace and business conduct when dealing with external parties. The manual also assisted in providing guidance on certain key issues such as bribery, conflicts of interest, insider trading and data integrity.

However, based on data provided by the fraud prevention and investigation department, which was accountable for investigation of suspected internal and external fraud cases, it was indicated that there was an increasing number of internal fraud cases reported from 2012 to 2013. This showed that, even though all documented policies and procedures were in place for all major aspects of the company's business, the employees remained unaware of the specific policies and procedures that they should comply with when they perform their routine tasks in the office.

The findings of all the cases show that, although good processes and procedures were established, if the processes and procedures were ignored or overridden, then internal control was paralyzed. Worse off, this provided opportunity for fraud to be committed, as shown in all the cases.

Two cases (case one and case three) relate a carelessness of the employee to adhere to procedures that provide opportunities for outsiders to commit fraud. In Case 1, the laziness of the employee to bring the laptop with her in attending the meeting outside the office, but left it in the car, is a big opportunity for the laptop to be stolen. It is general knowledge nowadays that electronic devices such as laptops, smartphones and GPS cannot be left in a car because thieves have devices to trace that kind of equipment and may break into a car, although such valuable equipment is not visible from outside the car.

In Case 3, the employee overrides the procedure by not performing proper identity verification on the consumer. The employee was defrauded by an unknown external party that requested customer information. Although no financial damage occurred, there is a possible risk of reputation damage, in which the consumer experiences a breach of trust and has the right to feel insecure because the company failed to protect their information. In other words, reputation damage can lead to loss of revenue because existing consumers may switch to competitors while at the same time find it difficult to attract new customers.

Cases 2 and 5 show poor supervision, one of the other important of internal control practices that can lead to abuse and misconduct. In Case 2, the supervisor poorly reacted to the verbal report of the loss of demonstration unit by the subordinate. Because of this, the subordinate did not care so much to take any serious effort to recover the phone. If fast action was taken by the supervisor, then other

Type of documents	Total
Divisional policy	44
Corporate policy	24
Operational policy	18
Standard operating procedures (SOP)	807

Table II.
Number of company policies and standard operating procedures

improvements could occur such as issuing instructions to all employees to increase their awareness when fraud occurs, informing security immediately for investigation. Case 5 revealed the failure of the supervisor to inform another unit regarding his subordinate resignation, which allowed his subordinate to perform unauthorized transactions for his advantage. Although no financial damage was suffered because this fraud was detected early, the loss of assets can incur in the future if a similar attitude was repeated by this supervisor. Implicitly, the courage of the subordinate to perform the unauthorized transactions was possible because of insufficient monitoring on his job by his supervisor, which he saw as an opportunity to commit fraud.

Case 4 is a clear fraud committed by the employee. She abused her position to collect money and made an adjustment to bill payment of her relatives. However, there is indication of poor internal controls because the employee admitted she knew well how the system works. Lack of job rotation may contribute to this fraud because, once the employee is an expert about a particular system, the employee may be able to manipulate that system's weaknesses for his or her advantage. Furthermore, the employee is able to conceal her fraud for a long time without being detected by anybody else. In addition, no segregation of duties and poor supervision are also possible in this case. There is no higher authority to verify and approve her work, that is, adjustment and update the customer's bill payment. Thus, the absence of checks and balances allow employees to have too much power, control and authority to make decisions.

Information and communication are other issues that surface from the cases. Almost all responsible employees were either not aware or never read about the specific policies and procedures shown to them. Nevertheless, after they were shown the document and went through the clauses in that particular document, they claimed that they understood and agreed with the policies. This shows that the level of awareness and comprehension among employees on the existence of relevant company policies and SOPs on internal fraud prevention is still at a low level. The message to the employees on the seriousness of control responsibilities did not arrive.

Conclusion

The purpose of this study is to determine the effectiveness of company policies and procedures on fraud prevention and examine whether employees are aware of and understand those policies and procedures. The study found that the company in this case study had sufficient policies, procedures and standards in which to prevent and detect fraud. However, human factors play an important part in ensuring the effectiveness of those policies and procedures. Poor attitudes toward overriding and ignoring the policies and procedures make the internal control systems dysfunctional. Insufficient supervision, lack of job rotation, lack of segregation of duties and broken communication also play their parts in motivating fraudsters.

The findings of this study confirm prior empirical research (Zakaria *et al.*, 2016; Omar *et al.*, 2016; Suhaimi *et al.*, 2016; Zhou, 2006; Bhattacharya and Marshall, 2012; Lisic *et al.*, 2014) and support the fraud triangulation theory (Cressey, 1973), which shows that opportunity because of poor internal controls and rationalization by assertion of not having awareness and understanding of the existence of policies and procedures motivates fraud. Therefore, it is crucial for a company to ensure effectiveness of the company policies and SOPs because, as in other organizations, opportunities and rationalizations for internal fraud to happen are always present.

This research has a few implications and recommendations to be adopted by a company to strengthen its internal control procedures. First, a company should communicate its attitude toward fraud. Top management should ensure that appropriate controls are established to prevent, detect and report fraud through effective means. As an example, strict actions should be taken on any major fraud that may adversely impact the company's image and reputation. The company should not tolerate any fraud and should require customers, employees, contractors, suppliers, business partners, dealers and other relevant parties to report any instances of fraud they may discover.

Second, company management, especially the human resources department, should ensure that ongoing and frequent awareness programs and training and education for employees are well executed. A sufficient budget should be allocated for those purposes. Through these means, employees are presumed to be familiar with the established policies and SOPs as well as understand their role in assisting the company to deter, prevent and combat fraud. Additionally, through training and awareness programs, employees are more likely to be alerted to the possibility that unusual events or transactions could result in fraud. Thus, they are immediately able to report details to their manager or immediate supervisor if they suspect that fraud or irregularities have been committed or if they see any suspicious events or acts.

Third, as the environment and company could both change, policies and SOPs must explicitly recognize the need to change in response, so they can work better under the new conditions. The company can use survey methods to obtain and evaluate feedback from those who use the policies and procedures and for determining whether existing policies and SOPs will continue to reflect reality and meet the company's goals.

Finally, relevant policies and standard operating procedures should be spelled out more specifically and give clearer explanations. For example, this study found that there were no specific policies and SOPs as guidelines in handling demonstration unit lost. This will indirectly contribute to the fraud and misappropriation of assets.

Limitation and suggestion for future research

As with other empirical studies, this study was subject to some limitations. First, this study only covers and examines internal fraud and wrongdoings, which were reported and investigated by the IO from the fraud prevention and investigation department over only two years. Future research should include more years and increase the number of cases so that different types of fraud and wrongdoing can be examined.

Second, the case studies were obtained at a single point of source, that is, staff. Future research could expand the scope of the study to include persons other than employees, such as contractors, vendors, suppliers, dealers and business partners.

Third, this study relies on only one method of data collection, which is content analysis of files and documents. Other methods of data collection, such as interviews and questionnaires, may be used in the future so that more issues and research questions can be examined.

Finally, as this study focuses on only one company and five fraud cases, the findings may not be generalized to other companies because of its different nature of business, culture, working environment, internal policies, control mechanisms and external conditions. Thus, future research should enlarge the number of cases, samples or firms that operate from various backgrounds and countries.

References

ActionFraud (2016), "What is fraud", available at: www.actionfraud.police.uk/what-is-fraud (accessed 31 January 2017).

Ahmad, N.M.N.N., Nawawi, A. and Salin, A.S.A.P. (2016), "The relationship between human Capital characteristics and directors' remuneration of Malaysian public listed companies", *International Journal of Business and Society*, Vol. 17 No. 2, pp. 347-364.

Asmuni, A.I.H., Nawawi, A. and Salin, A.S.A.P. (2015), "Ownership structure and auditor's ethnicity of Malaysian public listed companies", *Pertanika Journal of Social Science and Humanities*, Vol. 23 No. 3, pp. 603-622.

Association of Certified Fraud Examiners (ACFE) (2008), *Report to the Nations on Occupational Fraud and Abuse*, ACFE, Austin.

Association of Certified Fraud Examiners (ACFE) (2010), *Report to the Nations on Occupational Fraud and Abuse*, ACFE, Austin.

Association of Certified Fraud Examiners (ACFE) (2012), *Report to the Nations on Occupational Fraud and Abuse*, ACFE, Austin.

Bhattacharya, U. and Marshall, C.D. (2012), "Do they do it for the money?", *Journal of Corporate Finance*, Vol. 18 No. 1, pp. 92-104.

Bromley, D.B. (1986), *The Case Study Method in Psychology and Related Disciplines*, John Wiley & Sons, Chichester, Great Britain.

Cheng, H. and Ma, L. (2009), "White collar crime and the criminal justice system: government response to bank fraud and corruption in China", *Journal of Financial Crime*, Vol. 16 No. 2, pp. 166-179.

Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2013), *Internal Control—Integrated Framework*.

CPA Australia (2008), "Internal control for small business", available at: www.cpaaustralia.com.au/~/media/corporate/allfiles/document/professional-resources/business/internal-controls-for-small-business.pdf (accessed 31 January 2017).

Cressey, D.R. (1973), *Other People's Money*, Patterson Smith, Montclair, NJ.

Dilla, W.N., Harrison, A.J., Mennecke, B.E. and Janvrin, D.J. (2013), "The assets are virtual but the behavior is real: an analysis of fraud in virtual worlds and its implications for the real world", *Journal of Information Systems*, Vol. 27 No. 2, pp. 131-158.

Doyle, J., Ge, W. and McVay, S. (2007), "Determinants of weaknesses in internal control over financial reporting", *Journal of Accounting and Economics*, Vol. 44 No. 1-2, pp. 193-223.

Financial Reporting Council (2005), *Internal Control: Revised Guidance for Directors on the Combined Code*, FRC, London.

Free, C. and Murphy, P.R. (2014), "The ties that bind: the decision to co-offend in fraud", *Contemporary Accounting Research*, Vol. 32 No. 1, pp. 18-54.

Hamid, A.A., Haniff, M.N., Osman, M.R. and Salin, A.S.A.P. (2011), "The comparison of the characteristics of the Anglo-Saxon governance model and the Islamic governance of IFIs", *Malaysian Accounting Review*, Vol. 10 No. 2, pp. 1-12.

Hashim, M.F., Nawawi, A. and Salin, A.S.A.P. (2014), "Determinants of strategic information disclosure – Malaysian evidence", *International Journal of Business and Society*, Vol. 15 No. 3, pp. 547-572.

Hodson, R. (1999), *Analyzing Documentary Accounts*, SAGE Publications, Thousand Oaks, CA.

Husnin, A.I., Nawawi, A. and Salin, A.S.A.P. (2013), "Corporate governance structure and its relationship with audit fee – evidence from Malaysian public listed companies", *Asian Social Science*, Vol. 9 No. 15, pp. 305-317.

Husnin, A.I., Nawawi, A. and Salin, A.S.A.P. (2016), "Corporate governance and auditor quality – Malaysian evidence", *Asian Review of Accounting*, Vol. 24 No. 2, pp. 202 -230.

Jaafar, M.Y., Nawawi, A. and Salin, A.S.A.P. (2014), "Directors' remuneration disclosure and firm characteristics – Malaysian evidence", *International Journal of Economics and Management*, Vol. 8 No. 2, pp. 269-293.

Khadijah, A.S., Kamaludin, N. and Salin, A.S.A.P. (2015), "Islamic work ethics (IWE) practice among employees of banking sectors", *Middle-East Journal of Scientific Research*, Vol. 23 No. 5, pp. 924-931.

KPMG (2009), *KPMG Malaysia Fraud Survey Report*, KPMG Malaysia, Selangor.

KPMG (2010), *Fraud and Misconduct Survey 2010 – Australia and New Zealand*, KPMG.

KPMG (2013), *KPMG Malaysia Fraud, Bribery and Corruption Survey 2013*, KPMG, Selangor.

Leedy, P.D. and Ormrod, J.E. (2005), *Practical Research Planning and Design*, Pearson Merrill Prentice Hall, NJ.

Lisic, L.L., Silveri, S.D., Song, Y. and Wang, K. (2014), "Accounting fraud, auditing, and the role of government sanctions in China", *Journal of Business Research*, Vol. 68 No. 6, pp. 1186-1195.

Malhotra, N.K. (2010), *Marketing Research: An Applied Orientation*, Pearson Education, London.

Manan, S.K.A., Kamaludin, N. and Salin, A.S.A.P. (2013), "Islamic work ethics and organizational commitment: evidence from employees of banking institutions in Malaysia", *Pertanika Journal of Social Science and Humanities*, Vol. 21 No. 4, pp. 1471-1489.

Miller, R.L. and Brewer, J.D. (2003), *The a-Z of Social Research*, Sage, London.

Nor, N.H.M., Nawawi, A. and Salin, A.S.A.P. (2017), "The influence of board independence, board size and managerial ownership on firm investment efficiency", *Pertanika Journal of Social Science and Humanities*, Vol. 25 No. 3, pp. 1039-1058.

Ogneva, M., Subramanyam, K.R. and Raghunandan, K. (2007), "Internal control weakness and cost of equity: evidence from SOX section 404 disclosures", *The Accounting Review*, Vol. 82 No. 5, pp. 1255-1297.

Omar, M., Nawawi, A. and Salin, A.S.A.P. (2016), "The causes, impact and prevention of employee fraud: a case study of an automotive company", *Journal of Financial Crime*, Vol. 23 No. 4, pp. 1012-1027.

Paine, L.S. (1994), "Managing for organizational integrity", *Harvard Business Review*, Vol. 72 No. 2, pp. 106-117.

Puah, C.H., Voon, S.L. and Entebang, H. (2009), "Factors stimulating corporate crime in Malaysia", *Economics, Management and Financial Markets*, Vol. 4 No. 3, pp. 87-99.

PWC (2011), *Global Economic Crime Survey*, PWC, New York, NY.

Rahim, S.A.A., Nawawi, A. and Salin, A.S.A.P. (2017), "Internal control weaknesses in a cooperative body: Malaysian experience", *International Journal of Management Practice*, Vol. 10 No. 2, pp. 131-151.

Salin, A.S.A.P., Manan, S.K.A., Kamaluddin, N. and Nawawi, A. (2017), "The role of Islamic ethics to prevent corporate fraud", *International Journal of Business and Society*, Vol. 18 No. S1, pp. 113-128.

Securities Commission (2007), "Commission guidance regarding management's report on internal control over financial reporting under section 13(a) or 15(d) of the Securities Exchange Act of 1934", available at: www.sec.gov/rules/interp/2007/33-8810.pdf (accessed 31 January 2017).

Smith, M. (2015), *Research Methods in Accounting*, Sage, London.

Suhaimi, N.S.A., Nawawi, A. and Salin, A.S.A.P. (2016), "Impact of enterprise resource planning on management control system and accountants' role", *International Journal of Economics and Management*, Vol. 10 No. 1, pp. 93-108.

Vona, L.W. (2012), *Fraud Risk Assessment: Building a Fraud Audit Program*, John Wiley & Sons, NJ.

Zakaria, K.M., Nawawi, A. and Salin, A.S.A.P. (2016), "Internal controls and fraud – empirical evidence from oil and gas company", *Journal of Financial Crime*, Vol. 23 No. 4, pp. 1154-1168.

Zhou, C. (2006), "Revision of criminal law: responding to six common financial crime techniques", China Business News, January 1, p. 2.

Zikmund, W., Babin, B., Carr, J. and Griffin, M. (2012), *Business Research Methods*, Cengage Learning, South-Western, OH.

Further reading

Petrovits, C., Shakespeare, C. and Shih, A. (2011), "The causes and consequences of internal control problems in nonprofit organizations", *The Accounting Review*, Vol. 86 No. 1, pp. 325-357.

Corresponding author

Ahmad Saiful Azlin Puteh Salin can be contacted at: ahmad577@perak.uitm.edu.my