A Study on Fraud Prevention and Detection Methods in Sri Lanka

Peiris, G.K.H.[1], Aruppala, W.D.N.[2]

[1,2] Department of Accountancy, Faculty of Commerce and Management Studies, University of Kelaniya, Sri Lanka.

[1]kushanhpeiris@gmail.com, [2]dilini@kln.ac.lk

Abstract

Forensic accounting is emerging area in countries like Sri Lanka even though it came up many years ago. Corporate frauds have been increasing worldwide, emphasizing the needfulness of forensic accounting and it has become a great opportunity for accountants and other professionals to think beyond the traditional framework. This study examines the perception of accounting professionals regarding the occupational fraud prevention and detection methods and software used in Sri Lanka. The survey was conducted using hundred accounting professionals of Sri Lanka. The results reveal that password protection, external audits, bank reconciliations and internal control review are quite common in use while bank reconciliation, cash review and password protection are also highly employed methods to detect occupational frauds. However, fraud hotline, forensic auditing and forensic accountants are identified as the least used methods. Further, filtering software, virus protection and firewalls could be identified as the commonly used fraud prevention and detection software used in Sri Lankan context. Implementation of effective fraud preventing and detecting methods, software is highly recommended on preventing and detecting corporate frauds in Sri Lanka.

Keywords: *Occupational Frauds, Forensic Accounting, Fraud Detection, Fraud Prevention*

Correspondence: dilini@kln.ac.lk

ORCID of authors: Aruppala, W.D.N. - https://orcid.org/0000-0002-6206-6000

DOI: http://doi.org/10.4038/kjm.v10i2.7692

Introduction

Background of the Study

The fraud risk is a challenge to all organizations and individuals. Fraud is a concealed crime with those who commit fraud actively trying to avoid detection. Therefore, a proactive attention is vital in this regard. The concern about frauds has been increasing from the past in the global context elaborating corporate collapse such as Enron, WorldCom, Global Crossing, Tyco, etc. which led to wipe out a large amount of money of the value of stakeholders.

According to the Association of Certified Fraud Examiners (ACFE), the world largest anti-fraud organization and premier training and education provider in anti-fraud, one of the main categories to categorize fraud is the occupational fraud (Report to the Nations, 2020).

Over the past 24 months, in the global context, $42 billion loss was reported due to fraud and 47% of the respondents were experienced fraud, being the second highest reported level of incidents in the past 20 years (PriceWaterhouseCoopers; PwC, 2020). Many studies conducted by ACFE say that frauds and its impact are increasing day by day leading the economy to keep growing adversely. In a global study on occupational fraud and abuse, the median response according to the professional experience of the respondents who are from more than 125 countries, is that organizations lose 5% of their annual revenues due to fraud. To place their estimate in context, if that 5% loss estimate were applied to $90.52 trillion which is the estimated Gross World Product in 2019, it would result in a projected total global fraud loss of $4.5 trillion approximately each year (Report to the Nations, 2020).

Fraud has become more costly and a greater impact for small firms rather than large firms (Report to the Nations, 2020). The median loss per fraud case of a small organization amounted to $150,000 and in large organization, $140,000 (Report to the Nations, 2020). At small businesses, on the basis of per employee, losses from frauds may be as much as 100 times larger than large businesses (Association of Certified Fraud Examiners, 2004). The damage occurred from fraud does not limit to the direct monetary loss. Collateral damage may incorporate mischief to outer business connections and relationships, worker confidence, and moral. Some collateral impacts of fraud can be long term and cannot be quantified easily, for example, damage to the company reputation and brand (PwC, 2020).

Employees are led to commit frauds relying on the inability of management to check what is happening under their span of control due to difficulty and expensiveness to go through large number of transactions. Very often the in-depth record screening required to detect improprieties slows down business and operational processes and it consumes labour and financial (Albrecht and Albrecht, 2002). According to those researchers, “the cure becomes worse than disease” and have identified the need of better antifraud weapons to aid clients and employers by practitioners.

Fraud is prevalent and increasing due to rise in gains and rewards of committing frauds and decline in the risk of being caught and punished. While the advantages increase, many companies fail to prosecute fraud offenders, or they are not sternly convicted or inflicted punishments by the criminal justice system (Weisenborn et al., 1997). The growth in fraud cases and large amounts involved have motivated accounting and auditing regulatory bodies, government and other stakeholders to seek additional enhanced fraud prevention and detection methods.

Fraud prevention is typically the most cost effective way of reducing losses from frauds. According to the Fraud Examination (04th Ed; 2012), once a fraud is committed, there are no winners. Perpetrators lose because

they suffer humiliation and embarrassment and also legal consequences because normally they are first time offenders who have clean history in their employment. They must have to make payments for taxes and compensations and also there may have some penalties and other implications. Victims also lose because they lose not only the assets stolen but also incur legal costs, lost time, negative publicity and other adverse consequences. Furthermore, if the organizations do not deal severely with the offenders, a signal is passed that nothing serious happens to the perpetrators, increasing the likelihood of fraud by others.

Auditors and accountants are well aware about the ways of control to support in the process of fraud prevention. The problem changes from prevention to detection as long as internal controls do not exist and do not practice within the organization or if such controls are ignored (Weisenborn et al., 1997).

It would appear that fraud would be easy to detect due to training methods for auditing, the lack of complex concealments, and the increased number of fraud cases. In fact, even in cases involving blatant material misstatement of accounting records, fraud detection remains difficult. When the offenders hire supposedly independent auditors to become a part of the scheme, providing large rewards, detection becomes even more difficult. Most of the fraud cases are initially discovered by tips (Report to the Nations, 2020). Bunget and Dumitrescu (2009) emphasize that, in the course of auditor's duties, auditors make only 20% of detection of frauds. On the other hand, fraud investigation can be very costly.

In Sri Lankan context, some corporate financial accounting scandals such as, Government of Sri Lanka bond scam, Golden-Key fraud, Sakvithi Housing and Constructions (Pvt) Ltd deposit fraud, etc. were revealed, highlighting the necessity of increased concern on frauds. And it led to decrease confidence of the investors who were in the financial markets. The stakeholders who are interested in the fraud detection and prevention methods or the increased fraud cases are needed to be advocated by the results of effective investigations using appropriate political, economic, social and technological adoption undergone within that environment and the conditions.

Research Problem

Numerous organizational anti-fraud efforts are not suited to the current context and are superficial to some extent (Andersen, 2004). Further, KPMG's Fraud Survey (2003) reveals that, many organizations are trying various new approaches and means to fight against fraud.

However, most of them are not in use in current practice and many of them are obsoleted with the technological adoption.

Diverse means to battle fraud are being looked for by many organizations due to few limitations on red flag approach which is an assisting tool in fraud detection. Red flags are associated with fraud, but the association is far from perfect. It might restrain internal and external auditors from identifying other reasons that fraud could occur because it pays attention only on cues specifically identified (Krambia-Kardis, 2002).

Indeed, critics of Statements on Auditing Standards (SAS) 99, consideration of Fraud in a Financial Statement Audit issued in October 2002, point to its massive reliance on the red flags approach (Kranacher and Stern, 2004). And also many organizations have tried fraud detection strategies which were impractical (Wells, 2004). Prevention of fraud is a more feasible strategy as it is often difficult to recuperate losses occurred from fraud once they are discovered (Wells, 2004).

Many cases on occupational frauds are being discussed in Sri Lankan context during last decade. However it is not well disclosed the way of identifying and controlling such

frauds by the responsible parties and the authorities. Further researchers noticed that most of the Sri Lankan organizations don't employ proper mechanism of monitoring and preventing occupational frauds. However the discussion on implementing a proper mechanism on fraud detection and prevention is broadly discussed in different levels in private and public sector organizations.

Even though fraud detection and prevention has become a popular topic in Sri Lanka, there is a lack of research studies conducted and published in this regard. Thus, there is a gap of knowledge on perception of accounting professionals regarding the occupational fraud prevention and detection methods and software used in Sri Lanka.

Research Objective

Main objective of this study is to identify perception of accounting professionals regarding the occupational fraud prevention and detection methods and software used in Sri Lanka.

Significance of the study

The increase of frauds in Sri Lanka, especially corporate financial accounting scandals such as government bond issue, Golden-Key issue etc., implies that there is a significant need for research approaches that allow auditors and investigators to prevent and detect fraud. According to National Fraud Initiative Report (2018), UK government saves £300m in two years (April 2016 - April 2018) by preventing fraud and error with the involvement of Central Government's National Fraud Initiative (NFI). Most of the studies conducted in relation to fraud prevention and detection methods were based on the data from developed countries and there was no any studies based on Sri Lanka. Moreover the existing findings and literature do not address the expectations of the interested parties in the context of Sri Lanka.

The advantages consist of preventing use of outdated and ineffective methods and reducing fraud risk through implementing more effective fraud prevention and detection techniques sooner. Small companies as well as large companies can protect the financials and non-financials of the company by utilizing the findings of this study.

A good anti-fraud system should be within any kind of organization to face for the frauds increased. Findings of this study may provide a guidance to management on making decisions on which methods can be used within their companies with greater effectiveness.

The remaining sections of this paper is structured as follows. The next sections review empirical and theoretical literature on fraud detection and prevention. There after research methodology is discussed. Discussion on findings is presented following the methodology section. Final section discusses the results of the study while providing the conclusion.

Literature Review

ACFE identifies Occupational Fraud as a one type of fraud and defines as; "The use of one's occupation for personnel enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets" (ACFE, 2002). Occupational fraud results from the misconduct of employees, managers, or executives and it can be anything from lunch break abuses to high-tech schemes.

As per the Report to the Nations (2018) the ACFE categorizes three main types of occupational frauds such as (1) Asset misappropriations, (2) Corruption and (3) Fraudulent statements. This is also known as the Fraud Tree. (Appendix 01)

Occupational Frauds

Corporate frauds are growing widely around the world. While the corporate fraud cases

are growing, the percentage of those reported to the police has been declining in recent years due to untruthiness of police and legal system (Courtois and Gendron, 2020). Frauds are not just only increasing; it's also expensive. According to the Report to the Nation (2020), the study conducted by the Certified Fraud Examiners, contains 2504 cases of occupational fraud that were investigated during the period from January 2018 to September 2019 and the total loss occurred by those identified cases exceeded $3.6 billion. Asset Misappropriation schemes were by far the most prevalent form of occupational fraud, consisting 86% of reported cases with the least median loss of $100,000.

Financial statement fraud schemes comprised just 10% of the cases but created the largest median loss at $954,000. Corruption schemes dropped in the middle, arising in just over one third of reported incidences and resulting a median loss of $200,000. Occupational frauds are more likely to be discovered by a tip than by any other means. More than half of fraud reporting tips come from the employees in the victimized organization. Meantime, substantial number of tips used for fraud detection came from people outside the organization and they suggest that organizations should consider to promote on reporting mechanisms to outside parties especially to customers and suppliers.

For small businesses, occupational fraud is significantly a threat. According to the study conducted by ACFE (2018), the smallest organizations suffered the greatest median losses. Small businesses lost almost twice as much per scheme to fraud compared with the organizations which have more than 100 employees. Usually, these organizations have less anti-fraud mechanisms than their larger counterparts, increasing their vulnerability to fraud. As per the Report to the Nation (2020), approximately 89% of occupational fraudsters had never been charged or convicted of a fraudulent act, and 86% had never been punished or dismissed for fraud-related conduct by employer. The losses caused by men were nearly 72% greater than losses caused by women. Owners and executives were responsible for a small percentage of fraud cases but the median loss was around $600.000.

When it comes to developing countries, specially in the case of Sri Lanka, Central Bank of Sri Lanka (CBSL) bond scam was one of the major financial scandal resulting a loss of more than $11mn to the nation (Gunasekara, 2019). The communicated amount of debt to be accepted by the primary dealers was LKR 01 billion and finally accepted ten times larger amount than the originally communicated amount (LKR10 Billion) with 30 years of maturity period. And also the interest rate resulting from the auction was much higher than the rate indicated by the CBSL and the bond acquired company having some inside, privileged knowledge.

Fraud detection and prevention methods and their effectiveness

Methods to combat fraud

Both fraudulent financial reporting and asset misappropriation have become major costs for many organizations (James et al., 2006). The various techniques to reduce cost of frauds include but are not limited to fraud policies, telephone hot lines, employee reference checks, fraud vulnerability reviews, vendor contract reviews and sanctions, analytical reviews (financial ratio analysis), password protection, firewalls, digital analysis and other forms of software technology, and discovery sampling (Carpenter and Mahoney, 2001; Thomas and Gibson, 2003).

Organizations that have not been fraud victims tend to rely more on intangible prevention tools such as codes of conduct or fraud reporting policies while those that have suffered fraud have implemented more tangible measures such as whistle-blowing

policies and fraud prevention and detection training (PwC, 2003). ACFE emphasizes that internal control weaknesses were responsible for roughly half of frauds and all identified anti-fraud controls in their study were associated with lower fraud losses and quicker in detection.

Red flag method

Elliot and Willingham (1980) show that the law distinguishes between actual fraud which is done intentionally, and constructive fraud which is not done deliberately. By comparison to more violent crime, acts of fraud are often called white collar crime. Cottrell and Albrecht (1994) point out that violent crimes provide clear physical evidence of their existence, while fraud is often not directly observed as a criminal act. Edmonds says that it is difficult to distinguish occupational offenders from the others. The commonly used red flag approach was introduced by Albrecht and Romney (1986).

Several recognized practitioners and professionals have collected potential indicators of management frauds. Fraud cases which were shown by Catlett (1974) are the result of internal control breakdowns. As a result of management direction, collusion of officers or employees, neglect or a combination of these similar factors, these breakdowns occur. These kind of internal control breakdowns should be viewed as an indicator, and also opportunity for frauds.

There may have one or more symptoms in particular fraud cases. But it does not mean that a fraud has happened definitely base on having symptoms. However it represents the possible conditions related to fraud; they are cues that mean to signal an auditor to the likelihood of fraudulent activity (Krambia-Kardis, 2002).

In the article related to detection of financial statement misstatement, Groveman (1995) wrote that "The most frequent causes of audit failure appear to be inappropriate audit team reactions to various warning signals." Auditors should be skeptical and more investigative to identify the frauds when indicators appear and they need to ensure that it will not cause a material misstatement on the financial accounts.

Friedman (1995) advised the professions of management, accounting, and auditing to pay attention to warning signs which could signal frauds and auditors to be more skeptical on them. Coopers and Lybrand (1977) identified various indicators to raise suspicions and Robertson (1996) lists various management fraud indicators.

Albrecht and Romney (1986) conducted researches related to red flags to check the predictive capability of red flags which auditors could use to decide which red flags to use in their audits.

Pincus (1989) conducted a study using red flag questionnaires to assist auditors in determining the possibility of material fraud during an ordinary audit engagement. The study results showed that the questionnaires led to greater comprehensiveness and uniformity in data acquisition, but did not show that the use of questionnaires assisted in the fraud risk assessment.

In their analysis, Albrecht and Romney (1986) subjectively applied the 86 red flags used and tested on 30 known and unknown fraud cases. Sorenson and Sorenson (1980) prove that the red flag method is a cost-effective early warning system which can be used to detect management fraud. According to Groveman (1995), he says that the failure of audit is due to various reactions on warning signals and those warning signals must be considered by the auditor. According to Weisenborn (1997), there are few limitations in applying the red flag method in an organization and some researchers have mentioned that the red flag method or the approach is very subjective in nature based on the literature referred.

Though these limitations are available, the use of red flags during an audit may be beneficial. The auditor must keep in mind that these indicators are not absolute and have to act accordingly.

Red flags analytical review procedures

Many previous studies on techniques and methods of fraud prevention and detection have focused on "red flags." For instance, in a study of practicing auditors, Albrecht and Romney (1986) discovered that 31 inner control-related flags were deemed better predictors of fraud.

Loebbecke and Willingham (1989) used the approach of red flags to create another conceptual model to assess the likelihood of fraud and a survey tool was used to query 277 audit partners of a big 6 firm. They found that assessing internal controls of the client by an auditor is important in assessing the likelihood of fraud.

Pincus (1989) discovered that auditors who did not use red flag checklists performed in a greater degree those who did in an experimental setting. Auditors, who held different views and sentiments concerning the degree of fraud risk showed by different red flag indicators, were found in another study. Auditors who have different client experience were determined to own different perceptions of the importance of a given red flag indicator (Hackenbrack, 1993).

Chen and Sennetti (2005) apply a restricted, industry-specific strategic auditing lens and a logistical regression model to a matched sample of 52 computer companies charged with fraudulent Securities and Exchange Commission (SEC) financial reporting. For fraud and non-fraud companies, the model obtained a general forecast rate of 91%. Moyes and Baker (2003) conducted a survey of practicing auditors concerning the fraud detection effectiveness of 218 standard audit procedures. Results indicate that 56 out of 218 procedures were considered more effective in detecting fraud. In general, the most effective procedures were those yielding evidence about the existence and/or the strength of internal controls.

Fraud detection for small companies according to Fraud Examination Book 04th Edition

Out of several methods, CPAs can choose to penetrate data thickets to find the relevant bits of evidence required to discover and deter fraud. Practitioners must first consider the scope of the auditable data of the company, its available resources, and the expertise and qualifications of its personnel to be successful in implementing these methods. According to Albrecht and Albrecht (2002), deductive methods are usually easy and economical to implement but can lead to contradictory results. Auditors searching for fraud in data from smaller organizations should find the most of the following technology-based approaches, depending on deductive analysis which may be enough.

Discovery sampling

A form of attribute sampling which is expected zero error rate. This estimates the percentage of a population that possesses a particular characteristic or attribute. This method is used to know whether a population contains any error indicative of fraud. If a significant error or fraud is found in a sample, the sampling process is ceased and the error or fraud is investigated.

Data mining

The process of discovering patterns in big data sets involving methods at the intersection of machine learning, statistics and data base system. In other words data mining is the analysis step of the knowledge, discovery and data base.

Digital analysis

This is based on Benford's Law and tests for fraudulent transactions based on whether digits appear in certain places in numerical values in the expected proportion. Usually, a significant deviation from expectations takes place due to two conditions: (1) A person has added observations on a basis of not conforming to the Benford distribution. (2) Someone has deleted observations from a data set that does not comply with the Benford distribution (Durtschi et al., 2004).

Fraud Detection for large companies according to Fraud Examination Book 04th Edition

Auditors especially who work at larger entities can use the inductive methods to focus on situations that are particularly susceptible to deception for more precise results. Nonetheless, understanding which areas to address is not obvious and CPAs and others that use inductive analysis need to; understand the business, understand possible frauds that could occur, determine possible fraud symptoms, use queries to search corporate information systems for such symptoms and evaluate the symptoms found to see whether fraud or other harmless factors caused them.

But doing so includes customized programming and other special skills of an investigative team composed of at least these three members, one of whom should be a CPA: a business process specialist, a database programmer and an expert on fraud with required qualifications. (Albrecht and Albrecht, 2002)

Other Fraud Prevention and Detection Methods

Maintain a fraud policy

Each business entity ought to develop and keep up a fraud policy for managing and supervising employees. A corporate fraud policy, which a model or sample is available in ACFE, should be very unique from a corporate code of conduct or ethics. The fraud policy needs to be properly communicated and obtained a written acknowledgement from the employees that it was carefully read and understood.

Establish a telephone hotline

Though it is more common, a rather novel approach is using anonymous telephone hotlines (Holtfreter, 2004). A telephone hotline permits employees to provide extremely confidential information regardless of the fear of punishment that accompanies being a whistleblower (Pergola and Sprung, 2005). A subscription service offered by the ACFE can be identified as a third party hotline. This method is not only a cost effective and time saving detection tool but also it improves deterrence.

Employee reference checks

Prior to employment, organizations should conduct an employee reference check. An employee with a bad reputation and bad history of doing frauds schemes, may move from one organization to another. This technique will prevent hiring dishonest people. Information gathered from resumes and other ways, needs to be verified. Even after the first employment reference check, a second reference check is also needed after six months from the commencement date of the new employment. That is because, a fraudulent employee's former workplace may not have enough time to record the resigned employee's records during the initial search. This may be revealed by a second check.

Fraud vulnerability reviews

With a fraud vulnerability review, company's exposure to frauds can be disclosed. This consists an assessment of what assets are held and how they could be misappropriated. A vulnerability review assists to highlight most vulnerable assets in the organization. For example, confidential customer data and

financial information mostly in E-businesses. This is a proactive method of detecting frauds.

Perform vendor contract reviews

Proper review of company agreements and contracts can facilitate a warning of probable contract fraud, comprising kickbacks, bribery, or conflicts of interest by the employees. Contract frauds may involve a conspiracy between organizational personnel and a trade supplier or conspiracy among two or more merchants. Awarded contracts should definitely be inspected for reasonableness of the contracts. Such a review may disclose that bribes or kickbacks may be the reason for such awards.

Use analytical review

Fraud can adversely impact financial statement trends and ratios. Unpredictable and unusual patterns should be chased to find whether fraud could be the cause of deviation. By conducting financial analysis, existing associations that are not likely to present or the absence of associations that are likely to be present should be identified. Trend (horizontal) analysis, ratio analysis (vertical analysis or common size statements), budgetary comparisons, industry averages analysis, and review of general ledger and journal entries are some of the analytical review techniques.

Password protection

Although passwords are the most effective, efficient, oldest line of computer defense. Organizations should assure that only legitimate users have access to the computer network and associated data. The complexity with passwords is the inverse relationship between making the password effective and usable. Users will tend to write the password down, placing it at a risk, if its requirements are more complex (Gerard et al., 2004). Password should be a mix of letters, numbers and special symbols and also limited attempts should be given for users to enter the password. Biological features (i.e. biometrics) such as voiceprints, fingerprints, retina patterns, and digital signatures are becoming more cost effective in near future.

Firewall protection

Firewalls prevent unauthorized access to company information and can be used at the software level and hardware level. There are some programs (e.g., ZoneAlarm, Comodo, Tinywall, etc.) which coordinate internet related software programs, such as browsers, email, etc., at the software level. Basically hardware firewalls or routers prevent people from finding the connection of the organization to the internet. The internet connection is known as IP address and that is hidden by hardware firewalls so that hackers cannot find the access to the connection (Gerard et al., 2004).

When considering Sri Lankan context De Silva (2019) has conducted a study on fraud prevention and detection techniques in commercial banks in Sri Lanka. Further Tennakoon et al. (2019) also studied on real time credit card fraud detection using machine learning. Farther, Rathnasiri and Bandara (2017) has conducted a study to identify the perception of professional accountants on forensic accounting in Sri Lanka.

Thus, different countries, different researchers have used different methods to identify fraud prevention methods and software in different situations. Some of the well-known methods are being used by most of the researchers and those can be identified as commonly used fraud detection and prevention methods. Further, perception of accounting professionals regarding the occupational fraud prevention and detection methods and software are also vague in different countries. r, the researchers try to find whether those methods are being used in the case of fraud prevention and detection in Sri Lanka. Therefore, this study focuses on

identifying fraud prevention methods and software by examining the perception of accounting professionals.

Methodology

Sampling procedure

The population of this study is comprised of qualified accounting professionals who are engaging with corporate sector in Sri Lanka. All the professionals consist with at least one of the professional qualifications mentioned at Table I (Appendix 02) to be identified as accounting professionals.

Main purpose of selecting accounting professionals as the sample of this study is to get more accurate feedback as they have a better awareness of fraud prevention and detection methods and practices even among all the other professionals working at the accounting and auditing field in Sri Lanka. Further, as forensic accounting and auditing is an emerging discipline in countries like Sri Lanka the accounting professionals can be considered as the most suitable unit of analysis of this study. Accordingly based on convenient sampling method hundred (100) qualified professionals are selected to conduct this study.

Data Collection

Data is collected through a standard questionnaire developed and presented by Bierstaker et al. (2006). The first part of the survey questionnaire consists of the demographic factors such as gender, age, academic qualifications, professional qualifications, basic information on frauds etc. The second part focuses on the information related to the experience on frauds. The latter part is included the questions to gather the data related to the effectiveness of the occupational fraud prevention and detection methods and software and their usage within the company.

Findings and Discussion

The results of demographic data analysis include analysis of information on respondents' gender, age distribution, educational level, professional qualifications, period of working experience, industry, operations, etc.

Accordingly, 30% of the sample respondents are Financial Managers, 21% are Accountants, 18% are Executives, 15% are Manager-Audit and remaining 16% from Chief Financial Officers, Consulting analysts, Forensic Investigators and Audit partners.

Further 62% of the participants are male and 38% are female. Among them 56% represent the age category of 20 to 29, 25% represent from 30-39, 15% represent from 40-49 and the rest of 4% represent 50 and above age category.

Findings of industry classification which is performed based on the Global Industry Classification Standard (GICS), 36% respondents represent Retail industry, 25% from Food, Beverage and Tobacco industry, 18% from Capital Goods industry, 4% from Banks industry, 3% from Diversified Financials, Consumer Services, Real Estate, Telecommunication Services and Materials industries. Remaining 2% represent Insurance industry.

Further 37% of the respondents represent the companies which are publically held and other 63% is not publically held.

Table II (Appendix 03) presents the analysis of respondents academic and professional qualifications, years of experience and the scope of operation.

As types of occupational fraud, bribery, cash misappropriation, Inventory and all other assets misappropriation have high possibility to occur. Economic extortion has the least possibility to occur. Sales and procurement is the most critical function to occur fraud.

Internal audit department is responsible to report to BOD and CFO.

With the revenue moved up, the pressure placed on employees to meet organizational objectives also has risen. There was a 47% of likelihood of fraud in organization which the revenue is between LKR 250 million to LKR 01 billion, 36% of likelihood in organizations which the revenue is over 01 billion and 27% of likelihood in organizations which the revenue is below LKR 250 million. Around 32% of the survey participants indicated that their company had been a victim of fraud, nearly 61% indicated that their company had not been a victim of fraud and 6% indicated that they did not know whether or not their company was a victim of fraud. 42% of participants expected fraud to increase in the future, while 29% did not expect fraud to increase and remaining 29% did not know. 58% of participants indicated funding for fraud prevention training had increased over the last three years, while 35% said it remained the same and only 7% said it decreased.

However, only 38% indicated funding for the internal audit department had increased over the past three years, while 52% indicated internal audit funding had remained the same and only 10% stated it had decreased.

Further, Table V (Appendix 06) presents the different methods employed in fraud prevention and detection in Sri Lankan context whereas Table VI (Appendix 07) presents different software used in Sri Lankan companies.

When analysis fraud prevention and detection methods with the purpose of achieving research objective of this study, bank reconciliation, cash receives, password protection, external audits and internal control review and improvements can be identified as the most popular methods in Sri Lankan context. Further, inventory observation, fraud auditing, ethics training, increased attention of senior management and corporate code of conduct are also employed in this purpose.

Further, findings on software used in fraud detection and prevention presents, Filtering software, Virus protection and Firewalls as the commonly used fraud prevention and detection software used in Sri Lankan context. Further, data mining software, digital analysis, discovery sampling software, continuous auditing software, forensic software packages and financial ratio analysis software are also used in Sri Lankan companies.

Conclusion

This study examined the perception of accounting professionals regarding the occupational fraud prevention and detection methods and software used in Sri Lanka and as a result researchers could identify commonly used occupational fraud prevention and detection methods used in Sri Lanka.

The extent of usage of fraud prevention and detection methods was checked, and the result showed that majority of the sample was using the selected methods. And also password protection, external audits, bank reconciliations, cash reviews, and internal control review and improvement are commonly used to combat occupational frauds. However, fraud hotline, use of forensic accountants, use of ethics officers and employee counseling programs are less often used. Further, Filtering software, Virus protection and Firewalls could be identified as the commonly used fraud prevention and detection software used in Sri Lankan context.

Though the awareness of red flags is at a considerable level, the red flags are used as a supportive tool to conduct the other fraud detection methods. For example, when going through an investigation, red flags may appear and with that, the investigator can

further look into the case; cash review process is not properly monitored due to the too much trust on the cash handler.

Frauds are happening day to day in different forms or ways. Practitioners have to be vigilant not to get deceived and need to implement necessary controls. Therefore a proper internal control system should be within the company to minimize frauds without considering the size of the business. Most of the organizations are reluctant to invest in antifraud methods due to the expensiveness of those methods implementation and maintaining of them. However organizations need to implement at least deductive methods which require minimum resources to adopt to those methods to combat frauds. Quality of the business processes is increasing day to day and also forensic accounting and related fields are growing same as the other industries, with unique features.

Most of the businesses are moving to technology driven operations and with that, frauds can be occurred in comprehensive and complicated manner. Therefore technology driven organizations should increase the technological improvement in fraud prevention and detection process as well. There is a high trend towards frauds with the enhancement in technology and availability of it. But companies should aware about the upcoming trend and should obtain prevention strategies to mitigate the situation. That's because, prevention is much better than detection when it comes to occupational fraud.

Frauds are something which is inevitable. Attitudes impact to commit or not to commit fraud. Therefore, the controls, software may sometimes unable to control frauds. Therefore mainly organization should focus on developing loyal employees along with technology implementation. And also since attitudes cannot be taught, organizations should maintain a good environment so as to emerge positive attitudes which lead not to commit fraud and suppress negative attitudes which lead to commit frauds.

Employees should be rewarded for being genuine with the purpose of avoiding occupational frauds. Opportunities to commit fraud need to be identified and eradicated with proper internal control system. Making action on fraud cases may be a process which takes some time even years. This may be an impact to companies. However, organizations need to take actions avoiding future encouragements to commit fraud.

The current study contributes to the existing knowledge by providing a better understanding on existing fraud detection and prevention methods and software employed in Sri Lanka while bringing a discussion on commonly used methods in the world. So, the study provides a guidance to Sri Lankan accounting professionals to be more vigilant on this aspect. Further, findings of this study emphasize the importance of monitoring occupational frauds that destroy the good health of the organization.

This study can be further developed by selecting the professionals who involve in the field of auditing and forensic accounting to obtain more accurate and relevant results on the current context. The sample also need to be increased to obtain more accurate result to draw a realistic conclusion.

References

Albrecht, W.S., Albrecht, C.O., Albrecht, C.C., and Zimbelman, M.F. (2012). *Fraud Examination*, (4th ed.).

Albrecht, W.S., and Albrecht, C.C. (2002). Root out financial deception: Detect and eliminate fraud or suffer the consequences. *Journal of Accountancy*, 30-34.

Albrecht, W.S., and Romney, M.B. (1986). A red-flagging management fraud: A validation. *Advances in Accounting*, *3*, 323-33.

Andersen, S. (2004). Despite more rigorous compliance programs, corporate fraud still thrives. *Corporate Legal Times*, 1-6.

Apostolou, B., Hassell, J., Webber, S., and Sumners, G. (2001). The relative importance of management fraud risk factors. *Behavioral Research in Accounting*, *13*, 1-24. https://doi.org/10.2308/bria.2001.13.1.1

Association of Certified Fraud Examiners. (2002). *Report to the Nation*: *Occupational Fraud and Abuse.* Austin, TX.

Association of Certified Fraud Examiners. (2004). *Report to the Nation*: *Occupational Fraud and Abuse*. Austin, TX.

Association of Certified Fraud Examiners. (2018). *Report to the Nation*: *Occupational Fraud and Abuse*. Austin, TX.

Association of Certified Fraud Examiners. (2020). *Report to the Nation*: *Occupational Fraud and Abuse*. Austin, TX.

Bierstaker, J.L., Brody, R.G. and Pacini, C. (2006). Accountants' perceptions regarding fraud detection and prevention methods. *Managerial Auditing Journal*, 21(5), 520-535. https://doi.org/10.1108/02686900610667283

Blocher, E. (1992). *The Role of Analytical Procedures in Detecting Management Fraud*. Institute of Management Accountants, Montvale, NJ.

Bunget, O.C., and Dumitrescu, A.C. (2009). Detecting and Reporting the Frauds and Errors by the Auditor. Megatrend Rev. *6*, No.1, 279 – 291.

Calderon, T.G., and Green, B.P. (1994). Signaling fraud by using analytical procedures. *Ohio CPA Journal*, *53*, No.2, 27-38.

Carpenter, B.W., and Mahoney, D.P. (2001). Analyzing organizational fraud. *Internal Auditor*, April, 33-38.

Chen, C., and Sennetti, J. (2005). Fraudulent financial reporting characteristics of the computer industry under a strategic-systems lens. *Journal of Forensic Accounting*, *5*, No. 1, 23-54.

Coderre, D. (1999). Computer-assisted techniques for fraud detection. *The CPA Journal*, August, 57-63.

Courtois, C., and Gendron, Y. (2020). Why Corporate Fraud Repots are Down.

De Silva, P. O. (2019). Study of Fraud Prevention and Detection Techniques in Commercial Banks in Sri Lanka. 5th International Conference for Accounting Researchers and Educators (ICARE–2019), Department of Accountancy, Faculty of Commerce & Management Studies, University of Kelaniya, Sri Lanka.

Durtschi, C., Hillison, W., and Pacini, C. (2004). Effective use of Benford's law in detecting fraud in accounting data. *Journal of Forensic Accounting*, *5*, No. 1, 17-34.

Gerard, G., Hillison, W., and Pacini, C. (2004). Identity theft: the US legal environment and organisations' related responsibilities. *Journal of Financial Crime*, *12*, No. 1, 33-43. https://doi.org/10.1108/13590790510625043

Gunasekara, M. (2019). Bond Scam: Court issues notices on suspects (online). *The Sunday Times Sri Lanka*, 30 June. http://www.sundaytimes.lk/190630/news/bond-scam-court-issues-notices-on-suspects-356005.html.(accessed 30 August 2020).

Hackenbrack, K. (1993). The effect of experience with different sized clients on auditor evaluations of fraudulent financial reporting indicators. *Auditing: A Journal of Practice and Theory*, *12*, 99-110.

Holtfreter, K. (2004). Fraud in US organisations: an examination of control mechanisms. *Journal of Financial Crime*, *12*, No.1, 88-95. https://doi.org/10.1108/13590790510625070

Hylas, R.E., and Ashton, R. (1982). Audit detection of financial statement errors. *The Accounting Review*, *57*, No. 4,751-65.

Kaminski, K., and Wetzel, T.S. (2004). Financial ratios and fraud: an exploratory study using chaos theory. *Journal of Forensic Accounting*, *5*, No. 1, 147-72.

KPMG (1998). *KPMG 1998 Fraud Survey*. https://www.us.kpmg.com.

KPMG Forensic (2003). *Fraud Survey 2003*, Montvale, NJ.

Krambia-Kardis, M. (2002). A fraud detection model: a must for auditors. *Journal of Financial Regulation and Compliance*, 10, No.3, 266-78. https://doi.org/10.1108/13581980210810256

Kranacher, M.J., and Stern, L. (2004). Enhancing fraud detection through education. *The CPA Journal*, November, 66-67.

Lanza, R. (2000). Using digital analysis to detect fraud. *Journal of Forensic Accounting*, *1*, No.2, 291-6. https://doi.org/10.1108/02686900610667283

Loebbecke, J.K., and Willingham, J.J. (1988). *Review of SEC Accounting and Auditing Enforcement Releases*, working paper, University of Utah, Utah.

Loebbecke, J.K., Eining, M.M., and Willingham, J.J. (1989). Auditors' experience with material irregularities: frequency, nature, and detect-ability. Auditing: *A Journal of Practice and Theory*, *9*, 1-28.

Moyes, G., and Baker, C.R. (2003). Auditors' beliefs about the fraud detection effectiveness of standard audit procedures. *Journal of Forensic Accounting*, *4*, No.2, 199-216.

Pergola, C.W., and Sprung, P.C. (2005). Developing a genuine anti-fraud environment. *Risk Management*, *52*, No. 3, 43.

Peterson, B.K., and Buckhoff, T.A. (2004). Anti-fraud education in academia. *Advances in Accounting Education: Teaching and Curriculum Innovations, 6*, 45-67. https://doi.org/10.1016/S1085-4622(04)06003-1

Pincus, K. (1989). The efficacy of a red flags questionnaire for assessing the possibility of fraud. *Accounting, Organizations, and Society*, *14*, 153-63. https://doi.org/10.1016/0361-3682(89)90039-1

PriceWaterhouseCoopers (PwC) (2003). *Global Economic Crime Survey 2003*. http://www.PwCglobal.com/extweb/ncsurvers.nsf.

PriceWaterhouseCoopers (PwC) (2020). *Global Economic Crime and Fraud Survey*. https://www.PwC.com/gx/en/services/advisory/forensics/economic-crime-survey.html.

Rathnasiri, U. A. H. A. and Bandara, R. M. S. (2017). The Forensic Accounting in Sri Lanka "Perception of Professional Accountants". Kelaniya Journal of Management, 6(2), 68-82. http://doi.org/10.4038/kjm.v6i2.7546

Rezaee, Z., Crumbley, D.L., and Elmore, R.C. (2004). Forensic accounting education. *Advances in Accounting Education: Teaching and Curriculum Innovations, 6*, 193-231. https://doi.org/10.1016/S1085-4622(04)06010-9

Thennakoon, A., Bhagyani, C., Premadasa, S., Mihiranga, S., & Kuruwitaarachchi, N. (2019). Real-time credit card fraud detection using machine learning. In 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence) (pp. 488-493). https://ieeexplore.ieee.org/document/8776942

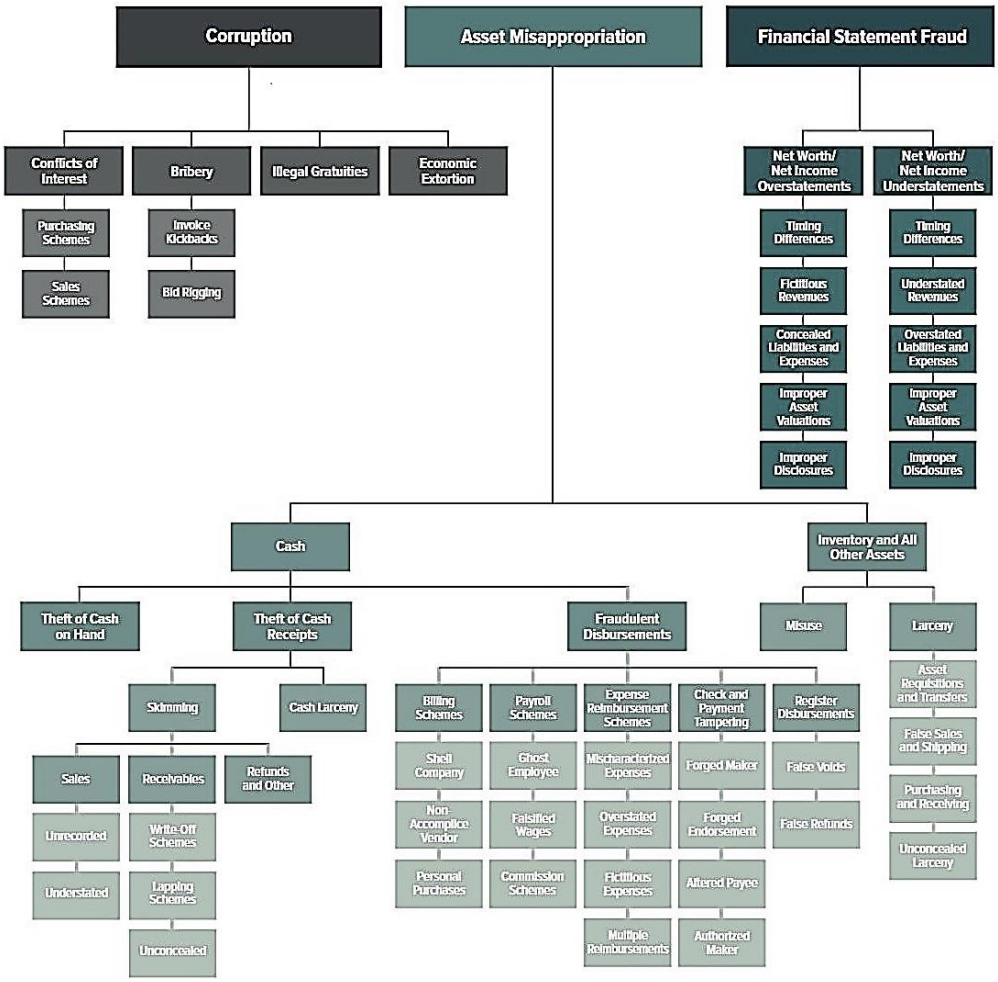
Thomas, A.R., and Gibson, K.M. (2003). Management is responsible, too. *Journal of Accountancy*, April, 53-55.

Wells, J.T. (2004). New approaches to fraud deterrence. *Journal of Accountancy*, *197*, 72-6.

Wright, A., and Ashton, R. (1989). Identifying audit adjustments with attention-directing procedures. *The Accounting Review*, *64*, No. 4, 710-28.

Appendices

Appendix 01



Source: Association of Certified Fraud Examiners. (2020). Report to the Nation: Occupational Fraud and Abuse.

Appendix 02

Table 01: Professional Qualifications considered to select the sample

ACA/FCA	Associate Chartered Accountant
ACCA	Association of Certified Chartered Accountant
CIMA	Chartered Institute of Management Accountants
CGMA	Chartered Global Management Accountant
CMA	Certified Management Accountant
CPA	Certified Public Accountant
CIA	Certified Internal Auditor

Appendix 03

Table 02: Significant Demographic Information

	Frequency	Percentage
Professional Qualification		
ACA/FCA	62	53
ACCA	9	8
CIMA	25	21
CGMA	9	8
CMA	6	5
Other	6	5
Academic Qualifications		
Master's Degree	23	23
Bachelor Degree	65	65
Advanced Level	12	12
Period of Experience (years)		
01-10	63	63
11-20	24	24
21-30	9	9
30+	4	4
Operations		
Local	49	49
International	4	4
Both	47	47

Appendix 04

Table 03: Normality test in the types of frauds related to the possibility of occurrence

Case processing summary		N	%
Cases	Valid	100	100.0
	Excluded	0	.0
	Total	100	100.0
Types of frauds related to the possibility of occurrence			Std. Error
Graph 01	Skewness	-0.339248	0.241380
	Kurtosis	-0.249857	0.478331
Effectiveness of fraud prevention and detection methods			
Graph 02	Skewness	0.047495	0.241380
	Kurtosis	-0.918397	0.478331
Effectiveness of fraud software			
Graph 03	Skewness	-0.483094	0.281029
	Kurtosis	-1.031733	0.555223

Appendix 05

Table 04: Reliability test in the types of frauds related to the possibility of occurrence

Case Processing Summary		**N**	**%**
Cases	Valid	100	100.0
	Excluded	0	.0
	Total	100	100.0

Reliability Statistics		**Cronbach's Alpha**	No. of Items
1	Types of frauds related to the possibility of occurrence	0.862	07
2	Effectiveness of fraud prevention and detection methods	0.978	25
3	Effectiveness of fraud prevention and detection software	0.980	09

Appendix 06

Table 05: Frequency and mean of fraud prevention and detection software

	Software Categories	Usage	Mean	
1	Virus protection	86%	5.30	(2)
2	Data mining software	46%	4.98	(4)
3	Filtering software	44%	5.36	(1)
4	Digital analysis	43%	4.59	(5)
5	Discovery sampling software	40%	4.40	(6)
6	Continuous auditing software	36%	4.38	(7)
7	Firewalls	30%	5.28	(3)
8	Financial ratios analysis software	28%	4.20	(9)
9	Forensic software Package	26%	4.23	(8)
	Overall	42%	4.75	

Appendix 07

Table 06: Frequency and mean of fraud prevention and detection methods

	Fraud Prevention and Detection Methods	Usage	Mean	
1	Password protection	100%	5.34	(3)
2	External audits	98%	5.26	(4)
3	Bank reconciliations	97%	5.52	(1)
4	Cash reviews	94%	5.49	(2)
5	Internal control review and improvement	94%	5.16	(5)
6	Reference checks on employees	94%	4.90	(11)
7	Inventory observation	91%	5.08	(6)
8	Increased attention of senior management	91%	4.95	(9)
9	Security department	91%	4.54	(16)
10	Employment contracts	89%	4.76	(12)
11	Corporate code of conduct/ethics policy	88%	4.91	(10)
12	Fraud reporting policy	84%	4.74	(13)
13	Code of sanctions against suppliers/contractors	83%	4.54	(17)
14	Fraud auditing	81%	5.03	(7)
15	Ethics training	81%	5.00	(8)
16	Surveillance equipment	75%	3.89	(23)
17	Staff rotation policy	73%	4.39	(19)
18	Increased role of audit committee	71%	4.33	(21)
19	Whistle-blowing policy	70%	4.47	(18)

20	Fraud vulnerability reviews	69%	4.63	(14)
21	Fraud prevention and detection training	65%	4.55	(15)
22	Employee counseling programs	59%	4.16	(22)
23	Ethics officer	44%	4.36	(20)
24	Organizational use of forensic accountants	38%	3.85	(24)
25	Fraud hotline	33%	3.81	(25)
	Overall	78%	4.71	