

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/286879136>

A fraud prevention policy: Its relevance and implication at a university of technology in South Africa

Article in *Journal of Governance and Regulation (online)* · December 2015

DOI: 10.22495/jgr_v4_i3_c2_p3

CITATION

1

READS

701

3 authors:



Amelia Nomfundo Rorwana

Tshwane University of Technology

4 PUBLICATIONS 8 CITATIONS

[SEE PROFILE](#)



Robertson K Tengeh

Cape Peninsula University of Technology

81 PUBLICATIONS 491 CITATIONS

[SEE PROFILE](#)



Tichaona Musikavanhu

Cape Peninsula University of Technology

3 PUBLICATIONS 3 CITATIONS

[SEE PROFILE](#)

Some of the authors of this publication are also working on these related projects:



The Influence of Culture on the Development of Youth Entrepreneurs in Selected Suburb in Cape Town [View project](#)



Job motivation and management implications [View project](#)

A FRAUD PREVENTION POLICY: ITS RELEVANCE AND IMPLICATION AT A UNIVERSITY OF TECHNOLOGY IN SOUTH AFRICA

Amelia Rorwana*, Robertson K. Tengeh*, Tichaona B. Musikavanhu*

Abstract

Using research grants administrators and their clients (academic researchers) as the lens, this paper investigated the relevance and implication of a fraud prevention policy at a University of Technology (UoT) in South Africa. The paper adopted a quantitative approach in which closed-ended questions were complemented by open-ended questions in the survey questionnaire in the attempt to capture the perceptions of both research grants administrators and their clients on the relevance and implications of a fraud and irregularity prevention policy. The results indicate that both research grants administrators (71.4 %), and their clients (73%) do not know if UoTx has a fraud and irregularity policy. While only 36% of research grants administrators indicated that they would feel safe reporting deceitful activities, a slight majority (59%) of the clients reported same. With regards to the steps to follow to report fraudulent activity, it was noted that while all (100%) the research grants administrators noted that they were clueless, ironically an overwhelming majority of their clients indicated otherwise. Notwithstanding, both research grants administrators and their clients (93% and 95% respectively) concurred that a fraud prevention policy was necessary for UoTx. The implication is that having phenomenal controls that are not effectively publicized, monitored or worse still overridden by someone are useless.

Keywords: Fraud Prevention, Research Grant Administrators, Financial Fraud, South African Universities of Technology

**Cape Peninsula University of Technology*

1 Introduction

Given that one of the core mandates of universities is to contribute to economic growth through research activities, Kriel (2003) notes that fraud and abuse of research funds have constituted a growing problem, preventing universities from delivering on that mandate in recent years. To forestall this trend, effective management becomes one of the pre-requisites. One aspect of the management process involves the prevention and an action plan against fraud and abuse. However, without clear guidelines, reporting procedures, and protection measures, administrators of research funds cannot contribute meaningfully towards curbing fraud and abuse of funds at universities.

1.1 Conceptualising the problem

Fraud losses impact on every organization with the associated costs passed on to society in the indifferent forms, including opportunity costs, unnecessarily high prices for goods and services, and criminal activities funded by the fraudulent gains (Wilhelm, 2004).

Fraud cost the African continent \$5.5 billion in the second half of 2012, with 75% of all fraud cases reported in Nigeria, Kenya, Zimbabwe and South

Africa (KPMG, 2013). This would translate to 5.5 billion /150000 (approximately 34000) tertiary education opportunities lost in South Africa. At least five universities have been placed under administration in South Africa in the last 3 years, and the common culprit here is fraud, and poor management among others.

Against the backdrop of the mismanagement of research funds, research administrators are expected to reconcile accounts and detect possible fraudulent activities. This is a challenging task, as there are fewer or no clear guidelines and procedures to follow. Research grant officers are therefore, uncertain of what to expect should they disclose fraud and abuse. Proactive universities have policies and procedures that facilitate disclosure. However, this cannot be said of UoTx. The aim of this paper is to investigate the relevance of a fraud prevention policy at UoTx in South Africa.

2 Literature review

2.1 Definition of fraud

The term fraud has different connotations to different schools of thoughts. For instance, Chui (2010) suggests that even scholars have established a long list

of guiding terms to simplify the meaning of the term fraud. According to Sitorus (2008) fraud is the act of corrupt practices encompassing financial crimes such as money laundering, and any other financial discrepancies conducted for personal fulfilment. Akers and Bellovary (2006) agree with the above view that fraud is an act of deliberately falsifying, misrepresentation and deceiving organizations in pursuit of personal gain.

In support of the above assertion, one draws from the work of Dycks, Morse and Zingales (2013). According to Dycks et al., (2013) fraud entails concealment, nondisclosure and misrepresentation. Thus, fraud entails a widespread of irregularities characterized by deliberate deception. Hence, Kochan (1992) perceives fraud to be the falsification of data for distortion purposes.

A similar view held by Harrison (2014) resonates with those held by other authors (Sirtorus, 2008; Chui, 2010; Dycks, et al, 2013), that fraud indeed is an act of dishonesty undertaken deliberately thus resulting in financial loss to the victim. In the context of this study, fraud is the act of unscrupulous practices committed against a higher education institution for personal fulfilment either by researchers or non-researchers. Having said that, one therefore, poses the

question: what type of fraud is committed by researchers and non-researchers? The following paragraph highlights the types of fraud committed in a university setting.

2.2 Types of frauds

There are several types of fraud being committed globally. Fraud can be categorized into mainly two groups. Jackson et al., (2010) postulate that there are two categories of fraud, which are financial statement fraud and occupational fraud. The authors described financial statement fraud as the misrepresentation the financial state of an organization, while occupational fraud is mostly committed by employees who steal items or money from a company. Bishop (2004) is of the opinion that there are three categories of frauds, which are potentially catastrophic frauds; costly but non-fatal frauds and insignificant frauds. However, Singleton & Singleton (2010) argue that there are many different fraud classifications and emphasize that fraud taxonomies should be able to be applied to antifraud programs, fraud investigations and antifraud controls. CIMA (2008) highlighted a more comprehensive taxonomy of frauds in figure1.

Figure1. Types of frauds

Fraud	Example (s)
Crimes against consumers, clients or other business people	Misrepresentation of quality of the products or services
Employee fraud against employers	Payroll fraud; falsifying expenses
Crimes by businesses against investors, consumers and employees	Financial statement fraud; selling counterfeit goods as genuine ones; not paying over tax contributions by staff
Crimes against financial institutions	Using lost or stolen credit cards; fraudulent insurance claims
Crimes by individuals or business against government	Grant fraud; tax evasion
Crimes by professional criminals against organizations (either SMEs or Large corporations)	Mortgage frauds; corporate identity fraud; money laundering
E-crimes by people using computers and technology to commit crimes	Spamming; copyright crimes; hacking; phishing; social engineering frauds

Source: adopted from CIMA, 2008:7

2.3 Types of fraud committed in the context of a university

Customarily, fraudulent activities and cases have been associated with business organizations (Omar, 2012; Jackson et al., 2010). However, there is considerable evidence today that educational institutions are also susceptible to fraudulent activities (JPMorgan, 2012). PWC (2012) concur with JPMorgan, but noted that institutions of higher learning do not publicize fraud cases due to fear of negative publicity. In 2014, the South African qualifications authority (SAQA) reported that there has been a growth in academic fraud among African countries. SAQA suggested that

Africa countries should collaborate to fight against qualifications forging related crimes (SAQA, n.d). The perpetrators of fraud in institutions of higher learning are both staff members and students, and in some cases they collude with third parties. These are some of the types of frauds committed in institutions of higher learning:

Misrepresentation of travel expenses: Is fraud committed by members of the academic staff who collude with the institution's travel supplier to increase (overstate) travel expenses (Hefce, 2015).

Misuse of purchase card: Purchase cards are given to staff members in some institutions to quicken the purchase of low value items. Some individuals

misuse these cards to cater for personal gains like buying personal gadgets which they do not record in asset registers (PWC, 2013).

Grant fraud applications: SABC (2014) recorded incidences of students falsifying documents required for them to apply for academic grant (NSFS), which was quoted to be a major drawback in funding efficiency in SA. Times higher education (1995) also noted some cases of individuals who intended to obtain grants by providing forged documents.

Examination fraud: PWC (2013) denotes that students are compelled to cheat due to industry pressure for good grades or fear of invalidation of international student visas. Students cheat in various forms, through bribing lecturers or gaining access to unauthorized examination papers, making other students to write their exam.

Non-formalized academic consultancy: This is another form of fraud when academic staff at institutions of higher learning conducts private consultancy using institution's equipment and time without seeking formal authorization (Hefce, 2015; JPMorgan, 2012).

Mandate fraud: Mandate fraud is when employees of an academic institution act as suppliers of a service or product in order to gain access of institution's funds. In this case the fraudster acts as a supplier (PWC, 2013). Hefce (2015) further highlighted that fraudsters can forge suppliers' bank details, either by diverting the paid figures into their accounts or increasing the costs after colluding with the supplier.

False academic and financial details: Guhr (2012) postulates that there has been a rise in students, especially international students who falsify their academic or financial support in order for them to be admitted in various international schools. Students falsify their transcript, financial support statements, recommendation letters, or test scores (SAQA, n.d; Guhr, 2012).

Impersonating a university to credit on goods: Hefce (2015) affirms that fraudsters uses institutional logos, and details to get goods or services on credit for personal gain. This is prevalent, where imposters target certain suppliers. JPMorgan (2012) also identified a similar case where individuals use email with higher education's institutions' name to solicit for funds from various organizations.

Use of stolen credit cards: This is a scenario where students make use of stolen credit cards to pay their tuition fees. Students buy or get credit cards from unscrupulous means, and use them illegally to pay for their academic fees (Hefce, 2015).

Fake award certificates: Senior academic staff issuing fake award certificates in return for financial favors (Hefce, 2015).

2.4 The effects of fraud on an organization

As previously noted, fraud is the misrepresentation of information for financial fulfillment. Therefore, when fraud is conducted in the context of an organization, an academic institution, financial institution or an insurance company, the most apparent result is financial losses. In fact, KPMG (2013) asserts that financial loss is the ultimate result fraud to any organization. CIMA (2008) further denotes that, the statistics on fraud is not easy to compile because a significant number of frauds go undetected or unreported.

At a very broad level, fraudulent activities have a significant impact on businesses (Omar, 2012; Jackson et al., 2010), and fraud is an unavoidable occurrence in organizations today (Gupta & Gupta, 2015; Omar, 2012). Organizations of all nature and size are not immune to fraud, from small and medium enterprises (SMEs) to large corporations, either profit or non-profit oriented organizations (Rahman & Anwar, 2014; Lowers, 2014; Singleton & Singleton, 2010; CIMA 2008; Greenlee et al., 2007). Furthermore, Singleton and Singleton (2010) highlight the preponderance of fraud at all levels of management including top managers, middle level, first line managers, and even employees. Lowers (2014) further noted that there are variations risks that occur in various organizations. The fraud tree model cited by Singleton and Singleton (2010) consider executive frauds to be the most expensive, though the least frequent. The most frequent frauds are committed by employees, but they are less costly compared to those of higher level management fraudulent activities.

Bierstaker et al., (2006) cited the Association of Certified Examiners (ACFE, 2004), who posited that about 6% of company revenues are lost annually due to fraudulent activities. The PricewaterhouseCooper (PwC, 2007) postulated that on average over a period of two years, UK companies lost 1.75 million euros (undetected fraud excluded). Another citation by CIMA (2008) of World Bank claims that corruption costs and bribery accounts for 5% of the global economy, which is about \$1.5 trillion dollars per annum. Fraud is said to be more severe on small companies than larger one (Bierstaker et al., 2006; CIMA, 2008). The authors further claim that, losses at small companies can be 100 times greater than that of larger companies, on the basis of per employee. Jackson, et al., (2010) shares the same views with Bierstaker et al., (2006) and CIMA (2008) that fraud is extremely destructive for small businesses, given that it accounts for a considerable proportion of failures Jackson et al., (2010) further note that small businesses have limited resources to recoup fraud losses. Regardless of the size, Gupta and Gupta (2015) assert that fraud leads to the untimely closure of businesses and destroys investor confidence.

Besides the monetary losses, Bierstaker et al., (2006) note that the collateral damage of fraud can be severe, in such that it:

- Causes harm to external relationships with various stakeholders
- Can reduce employee morale
- Can tarnish organization's reputation
- Can hinder the effectiveness of organizational branding

The effects of fraud can be permanent (Bierstaker et al., 2006). Fraud inflicts psychological and social effects on individuals and companies. This is supported by CIMA (2008) who posited that fraud can cause company closure, with the resultant loss of income and source of living for many people who depend on the organization. In the quest to recoup money lost from fraud, organizations pay a considerable amount of money to investigate and stabilize the organization (CIMA, 2008). Singleton and Singleton (2010) suggest that losses due to fraudulent activities are difficult to recover, though they suggest that entities should develop strategies for recovery.

2.5 Prevention of fraud

Fraud remains a sensitive issue across every sector of business, whether public or private businesses. As a result, a considerable proportion of businesses are vulnerable to fraud and misconduct. Hence, it is critical to rather prevent fraud than to nurse the effects of fraud. Though fraud can be prevented in numerous ways, a pertinent solution in organization would be a policy that vigorously deals with fraud prevention measures (Wilhelm, 2004). As such one may argue that fraud can be best prevented through policy and monitoring. Recovering from fraud is costly and time consuming; therefore preventing fraud from occurring or limiting the occurrences will enable an organization to maintain the sustainability path.

Omar (2012) asserts that various organizations have emphasized on detecting fraudulent activities rather than preventing them from occurring. The author suggests that, organizations should rather focus on prevention and deterrence to eliminate or reduce the opportunity of fraud from occurring. Bishop (2004) stands on the view that different types of frauds should be treated differently. Furthermore, Omar (2012) upholds that fraud prevention should be the responsibility of the entire organization.

Singleton and Singleton (2010) argue that to counter fraud activities, fraud principles become the epicenter of a fraud policy, investigating a fraud or designing anti-fraud controls. Antifraud programs should prevent fraud, and not just detect it. These authors further argue that, though detecting fraud is vital, prevention is preferable. In the same line, CIMA (2008) adds that organizations should invest strategic resources and time in tackling fraud. Rahman and Anwar (2014) contend that although there is a dire

need to eliminate fraud, there is no ultimate solution to fraud. This notwithstanding, it is imperative that a number of different methods and techniques should be simultaneously used or integrated to help to combat fraud. Preventive measures reduce opportunity and temptation from potential offenders (CIMA, 2008). Moreover, Singleton and Singleton (2010) posit that it is essential to understand why fraudsters commit fraud, which then enables effective prevention measures to be crafted. There are three fundamental causes of fraud are: (1) pressure, which could be a strong desire to be successful; (2) opportunity, that could be a weak area of an organization or (3) rationalization that is individual justifications of dishonest actions (Gupta & Gupta, 2015; Jackson et al., (2010). Omar (2012) affirms that understanding the root cause of fraud and the use of effective fraud prevention methods is vital in reducing financial fraud incidences.

Rahman and Anwar (2014) and Jackson et al., (2010) note that fraudsters use modern-day technologies and tools, which makes fraud complex and difficult to detect or prevent, despite concerted investments in technologies that organizations make to counter these fraudulent activities. Rahman and Anwar (2014) further suggest a number of effective fraud prevention strategies that organizations can choose from including:

Fraud policy: Fraud policy is an effective tool for preventing fraud (Taylor, 2011; Singleton & Singleton, 2010). The policy should be communicated to the employees through the use of employee orientation programs, employee handbook and on regular meeting or scheduled training sessions. Furthermore, Singleton and Singleton (2010) highlighted that definitions of fraud should be clarified to avoid ambiguity among employees, because there are many definitions of fraud. Lowers (2014) affirms that communication about from top management to low level management is essential and trainings helps to create transparency and enhances anti-fraud implementation efficiency. If consumers understand appropriate behaviors, it impedes them to rationalize inappropriate behaviors (Jackson et al., 2010).

Telephone hotline: telephone hotlines have become very useful and cost-efficient tools to prevent and detect suspicious fraudulent activities in various organizations (Rahman and Anwar, 2014; CIMA, 2008; Bierstaker et al., 2006). Internal or external sources can anonymously report any suspicious activity either to a third party who provides hotline services or can be done within an organization (Omar, 2012; Bierstaker et al., 2006). Rahman and Anwar (2014) argue that, the use of hotline is not an effective tool but serves as a deterrent. CIMA (2008:30) asserts that the challenge that organizations have is to encourage individuals to report any potential malicious acts. Furthermore, CIMA (2008) provides solution that organization cultures that upheld openness can overcome the culture of silence. Omar

(2012) postulated a view that anonymous hotline can be a source of positive work environment which in turn reduce pressure or motive to commit fraud.

Exit interview: Employees who are leaving an organization might have valuable information that can be used to combat fraud (Lowers, 2014). The challenge that employers have is to encourage them to speak of fraudulent activities or potential occurrence.

Employee reference check: Taylor (2011) posits that employee reference check enables HR managers not to employ dishonest employees. Reference checks or background checks should be done on all prospective employees (Jackson et al., 2010; CIMA, 2008; Bierstaker et al., 2006). These checks include confirmation of educational qualifications, verifying previous employment background and scrutinizing CVs. Lowers (2014) affirms that potential employees with high probability to committing fraud should be eliminated during the recruitment process.

Fraud vulnerable review: fraud vulnerable review enables organization to assess susceptible area in an organization of how fraud can be committed and what probably measures can be put in place to combat it (Bierstaker et al., 2006). CIMA (2008) denotes that fraud risks assessments can be done in terms of likelihood and impact either monetary value or non-monetary value. Additionally, Bierstaker et al., (2006) assert that the review is done to outsmart fraudsters or potential crooks. The reviews also help to channel the focus for internal audit plans.

Password protection: Rahman and Anwar (2014) and Lowers (2014) assert that the use of passwords prevents unauthorized access to certain confidential information for non-privileged users. Bierstaker et al., (2006) postulate that internet has been invariable been used as a trading platform by various companies across the globe, the use of password deter illegitimate users form gaining access to unauthorized information. Various companies uses passwords creation criteria which helps to bar hackers, furthermore biometric passwords have also gain prominent (that is the use of fingerprints, voiceprints, digital signatures etc (Rahman & Anwar, 2014; Bierstaker et al., 2006).

Continuous auditing: Continuous auditing can be done through the use of computer technologies, which constantly or regularly monitor transactions (Rahman & Anwar, 2014). Continuous auditing helps to detect imminent fraudulent activities, rather than auditing historical data (Rahman & Anwar, 2014; Lowers, 2014).

Digital analysis: Bierstaker et al., (2006) is of the view that digital analysis enables detection of figures that do not align with the Benford's Law. If errors signifies that figures were modified or tampered with. Although, this method has its drawback, it has been widely used.

Discovery sampling method detects errors in information. The expected error rate is zero, but if there is any error rate besides zero, that is an

indicative of prospective fraudulent activity (Bierstaker et al, 2006). The method is also deemed efficient in detecting fraudulent activities within an organization.

2.6 What is a fraud prevention policy?

The department of the national treasury of the republic of South Africa provides a framework for fraud prevention policy (National Treasury, n.d). The policy provides guidelines for the reduction and possible eradication of fraudulent activities and other misconduct within organizations. Singleton and Singleton (2010) assert that fraud policy is an essential tool in an antifraud program.

2.6.1 The importance of a fraud prevention policy

Fraud policy is a useful preventative measure against fraud. The policy provides guidelines on how to prevent, detect and respond to fraudulent activities within an organization (Lowers, 2014; Taylor, 2012; Singleton & Singleton, 2010).

Taylor (2011) makes reference to 5 fundamental elements of the policy which are:

- An agreement to the adherence to organization ethical and moral values which should be signed by employees
- The role and attitude of the board to fraud and illegal behaviour
- Who the policy applies to
- What actions are defined as fraudulent, (i.e. include bribery and corruption, deliberate misrepresentation, theft, etc.).
- The board's policy towards fraud and the actions it intends to take where instances of fraudulent or corrupt behaviour are discovered.

2.7 Who are research grant administrators?

Research administrators are professional individuals who are trained or qualified to administer research funds, and they also support researchers, by sourcing funds from various bodies (Kulakowski & Chronister, 2006). These individuals also play a vital role of assessing the value of various interdisciplinary researchers, examining their feasibility within the institutional capacity to sponsor and manage them.

Research administrators ought to be well versed with knowledge from different spheres of studies and have the ability to determine value adding researches. Often, research administrators are synonymous with intermediary, brokers and/or helpers. However, their main roles as mentioned by Kulakowski and Chronister (2006) are:

- Understand the nature of the of the principal investigators (PI)'s research
- Assist PI with pending funding opportunities information

- Promote a positive relationship between the PI and the research sponsors
- Helping the PI apply for a grant or contract, especially through assistance with budget, approvals etc.
- Ensuring that the PI research proposal comply with institutional policies and sponsor requirements
- Assisting the PI with the financial and managerial aspects of awards
- Ensuring the integrity of the institution's financial and non-financial processes related to the research function.

Across the globe, there are various professional bodies that train research grant administrators, for example RACC (Research Administrator Certification Council - <http://www.cra-cert.org>). These organizations certify individuals who would want to pursue a research administration career. The various individuals who would have been certified by this body are deemed to have acquired relevant knowledge and expertise to assume the position of a professional research or sponsored programs administrator (RACC, n.d).

The research grant administrator should be equipped with (1) the ability to find meaning in both qualitative data or quantitative data, (2) they should be good communicators at a level, (3) good problem solvers, (4) should be professionally equipped with research administration skills, (Kulakowski & Chronister, 2006).

3 Method

The paper adopted a quantitative approach in which the closed-ended questions were complemented by open-ended questions, to capture the perceptions of both research-grants administrators and their clients (researchers) on the relevance and implications of a fraud and irregularity policy.

Questionnaires are undoubtedly one of the primary sources of obtaining data in any research initiative. Nonetheless, it is commendable that when designing a questionnaire, the researcher should ensure that it is "valid, reliable and unambiguous" (Richards & Schmidt, 2002). According Zohrabi (2013), questionnaires can generally group into three types: closed-ended; open-ended, and a mixture of closed ended and open-ended questionnaires.

Closed-ended questionnaires provide the inquirer with quantitative or numerical data and open-ended questionnaires with qualitative or text information (Zohrabi, 2013). Close ended questions have been criticised for being biased in that they suggest and limit the respondents' responses (Reja, Manfreda, Hlebec & Vehovar, 2003). To avoid the inherent bias associated with closed-ended questions, open-ended questions were utilized. This thus added an element of the qualitative approach. Open-ended questions also known as narrative open-ended questions have been particularly praised for providing the researcher the opportunity to gain detailed spontaneous responses and to explore new topics where exhaustive answer

categories cannot be provided (Reja, et al, 2003; Zohrabi, 2013). The open-ended questions were treated as qualitative data.

One hundred (100) questionnaires were emailed to academics randomly that drawn from a compiled database of active researchers. From this number, 44 questionnaires were returned, presenting a 45% response rate. Another set of questionnaires was administered all the research grants administrators presenting all the faculties in the university. All twelve research grants administrators on this data base were reached, thus represented a 100 % response rate.

The e-mail survey method of data collection was the preferred. The constructed questionnaires were pilot-tested and deficiencies were addressed accordingly. The survey questionnaire was then mailed to each respondent with a cover letter explaining the purpose of the survey. Descriptive analysis techniques were used to analyse the survey data.

3.1 Delineation of this paper

In the context of this paper, fraud in university was limited to financial fraud. The sample was limited to research grants administrators and active academic researchers. The content of a fraud prevention policy was not the primary concern.

4 Results and discussions

The results are presented and discussed in the following section.

4.1 Gender of the research participants

Figure 1a and 1b, illustrate the gender profile of the participants. It is evident from figure 1a that the majority (71%) of grant administrators were female, while 29% were males. Responding to the same question, it was noted that 63% of the research respondents were male while 36 were female.

Figure 2a, highlights that 71.4% of research grants administrators do not know if UoTx has a fraud and irregularity policy, while 28.6% agree that UoTx has a fraud policy. Responding to the same question, while the overwhelming majority (73 %) of the academic researchers surveyed indicated that they were not aware of a fraud and irregularity policy at UoTx, 29 % noted the reverse. A follow up open ended question required that the participants elaborated on their awareness of the fraud and irregularity policy at UoTx. Some sample direct responses from the participants (researchers) include the following: "... As a researcher, I assume there should be one since it is a requisite for many grants".

"... I have not had to use it".

"... I do not know anything more about it".

"... I have never had the opportunity to peruse it".

"... Through a mail policy document and whistle blowers - online system".

Figure 1a. Research administrators

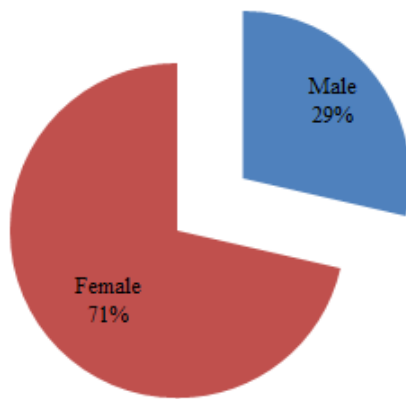
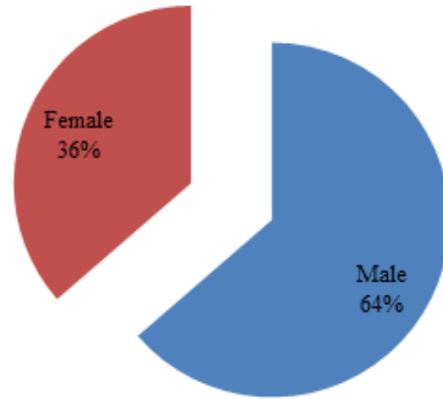


Figure 1b. Academic Researchers



4.2 Awareness of a fraud and irregularity policy?

Figure 2a. Research administrators

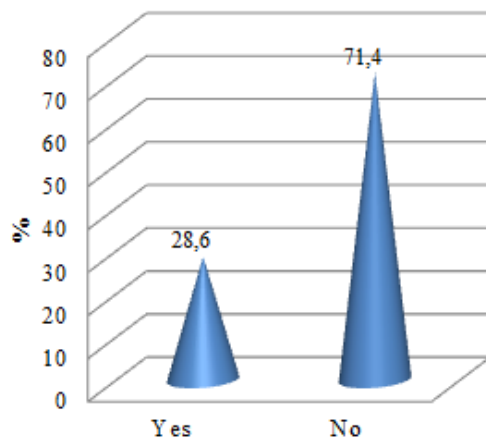
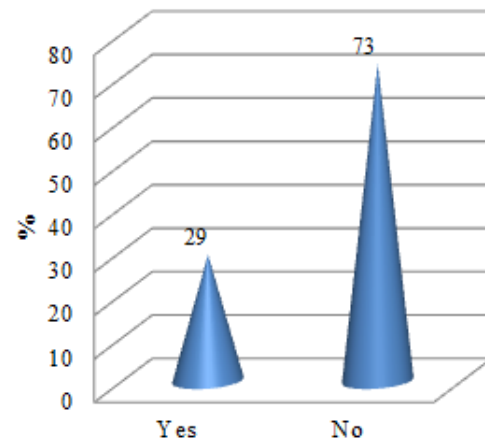


Figure 2b. Academic Researchers



4.3 Safety in reporting fraudulent activities

Figure 3a and figure 3b illustrate the respondent's perceptions on how safe it is to report research funding irregularities.

Figure 3a. Research administrators

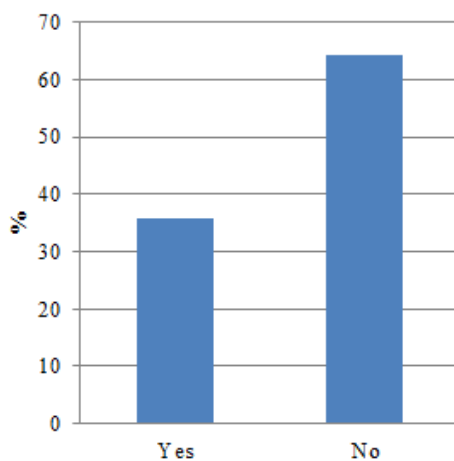
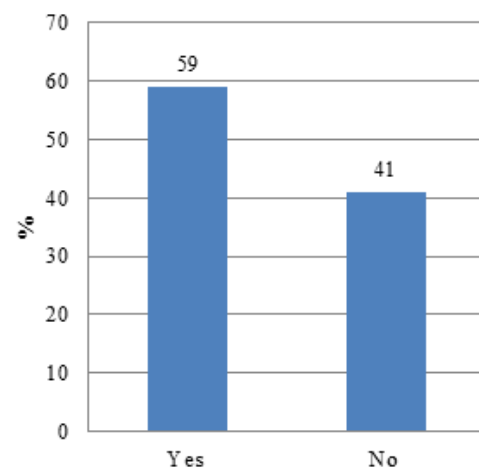


Figure 3b. Academic Researchers



With specific reference to research grant administrators, figure 3a illustrates how safe whistle-blowers feel about reporting any mismanagement of research funding. Thirty-six percent (36%) of respondents reported that they feel safe to report mismanagement of the research funds while the 64% reported that they do not feel comfortable to report. Turning to their clients (researchers), it was highlighted (figure 3b) that while 59% noted that they felt free to report fraudulent activities, 41 % felt otherwise.

4.4 Steps to follow when reporting abuse of research funds

Responses to the question of whether respondents know the steps to follow when reporting research funding abuse, that all (100%) the research grants noted that they do not know the procedures to take to report irregularities. Turning to academic researchers,

an overwhelming majority (97%) revealed that they know the steps to follow in reporting fraudulent activities. However, a significant minority (3%) indicated their ignorance with regards to the steps to follow to report fraudulent activities.

The foregoing results tend to be contradictory. While, on the one hand, the research grant administrators who are tasked with issuing and reconciling research funds claim that there are no clear guidelines on how to report fraud, on the other hand, their clients indicate the contrary. Drawing from the works of Taylor (2011) and Singleton and Singleton (2010) one may argue that if a policy exists, it needs to be thoroughly communicated to the employees through the use of employee orientation programs, employee handbooks and at regular meetings or scheduled training sessions.

4.5 Would you like UoTx to have fraud and irregularity policy?

Figure 4a. Research administrators

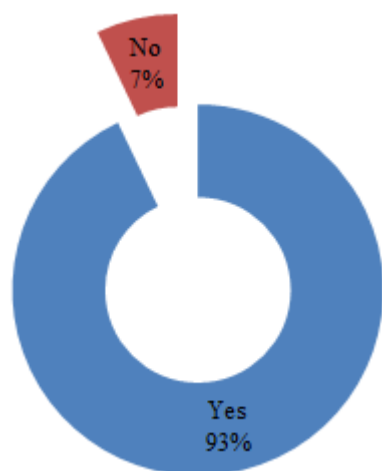
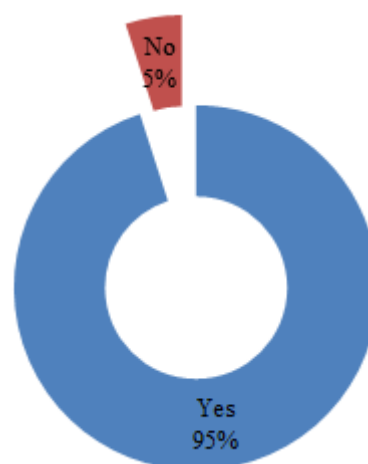


Figure 4b. Academic Researchers



When asked whether a fraud and irregularity policy was necessary for UoTx, it was reported by the overwhelming majority (95 %) of the academic researchers such a policy is a must. A number of reasons not limited to, the following were advanced in support of a fraud and irregularity policy:

- ... As it will highlight the seriousness that senior management takes fraud seriously
- ... Colleagues should be trustworthy not to commit fraud, otherwise we fail as a society.
- ... Fraud in research funding puts at risk future availability of such funding.
- ... It is always good to have a policy that spells out the process and consequences
- ... This helps to ensure that researchers are ethical and it promotes proper use of research funds.
- ... To curb irregularities and to ensure fairness to all researchers who need money for research.
- ... To know how to report such incidences safely

- ... To prevent fraud and misuse of research funds

- ... It is a prerequisite of many funders.

The findings noted above align with the need to prevent rather than deal with the aftereffects of fraud (Omar, 2012). Thus, organisations should rather focus on prevention and deterrence to eliminate or reduce the chances of fraud occurring.

5 Conclusion

Against the backdrop of increasing mismanagement of research funds, research administrators are expected to reconcile accounts and detect possible fraudulent activities. This is a challenging task, as there are few or no clear guidelines and procedures to follow. Research grant officers are therefore, uncertain about what to expect should they disclose fraud and abuse. It was revealed that there are not clear policies on how to report fraud and to whom this is compounded by a lack of protection assurance to the disclosers.

Universities should recognize that excellence in research requires sound proactive management practices. Excellence in research and sound university management are concomitant with good financial management, but despite its ubiquity, fiscal crime can be prevented by a clear policy detection of fraud and abuse that offers protection to disclosers. As contended by Schwartz et al. (2008), “You can have phenomenal controls, but they would not work if someone overrides them”. The implication is that having phenomenal controls that are not effectively publicized, monitored or worse still overridden by someone are useless.

References

1. Akers, M & Bellovary, J. (2006). What Is Fraud and Who Is Responsible? *Journal of Forensic Accounting*, 7(1): 247-256.
2. Bierstaker, J.L., Brody, R.G. & Pacini, C. (2006). Accountants' perceptions regarding fraud detection and prevention methods. *Managerial Auditing Journal*, 21 (5): 520 – 535
3. Bishop, T.J.F. (2004). Preventing, deterring, and detecting fraud: What works and what doesn't. *Journal of investment compliance*, 5 (2): 120-127.
4. CIMA . (2008). Fraud risk management A guide to good practice http://www.cimaglobal.com/documents/importedddocuments/cid_techguide_fraud_risk_management_feb09.pdf.pdf [Accessed 01.06.2015].
5. Chui, L. (2010). An experiential examination of the effects of fraud specialist and audit mindset on fraud risk assessments on the development of fraud-related problems representations. Unpublished PhD thesis. University of North Texas.
6. Dyck, A., Morse, A. & Zingales, L. 2013. How pervasive is corporate fraud. Available at <http://ssrn.com/abstract=2222608> (accessed 05/03/15).
7. Greenlee, J., Fischer, M., Gordon, T., & Keating, E. (2007). An investigation of fraud in nonprofit organizations: Occurrences and deterrents. *Nonprofit and Voluntary Sector Quarterly*.
8. Guhr, D. (2012). Fraud in international education – The tip of the iceberg. <http://www.universityworldnews.com/article.php?story=20120210094015109> [Accessed 06.06.15].
9. Gupta, P. K., & Gupta, S. (2015). Corporate frauds in India-perceptions and emerging issues. *Journal of Financial Crime*, 22 (1): 79-103.
10. Harrison, A.J. (2014). The effects of technology on interpersonal fraud. Unpublished Master's thesis. Iowa State University.
11. Hefce. (2015). Notifications. <http://www.hefce.ac.uk/reg/Notifications/Fraud,updates/>. [Accessed 06.06.15].
12. Jackson, K., Holland, D. V., Albrecht, C., & Woolstenhulme, D. R. (2010). Fraud isn't just for big business: understanding the drivers, consequences, and prevention of fraud in small businesses. *Journal of International Management Studies*, 5 (1): 160-164.
13. JPMorgan. (2012). Mitigating payment fraud risk: Strategies and best practices for higher education institutions. <https://www.jpmorgan.com/cm/BlobServer/JPM-MitigateFraudRisk-HigherEducation.pdf?blobkey=id&blobwhere=1320603368619&blobheader=application/pdf&blobheadname1=Cache-Control&blobheadervalue1=private&blobcol=urldata&blobtable=MungoBlobs> [Accessed 06.06.15].
14. Kiel, C.J. (2003). Duty of disclosure of fraud and abuse in research administration. Society of Research Administrators (SRA) Symposium: 87-96, Pittsburgh, Pennsylvania, October 18-22.
15. Kochan, C.A. & Budd, J.M. (1992). The persistence of fraud in the literature: the darsee case. *Journal of the American society for information sciences*, 43(7):488-493.
16. KPMG, (2013). 3rd KPMG Africa Fraud Barometer. KPMG International.
17. Kulakowski, E.C. & Chronister, L.U. (2006). Research administration and management. Jones & Bartlett. London. https://books.google.co.za/books?id=NCFYnrS_nVwC&printsec=frontcover&source=gbs_atb&hl=en#v=onepage&q&f=true [Accessed 04.06.15].
18. Lowers, M. (2014). Key components of a fraud prevention policy. <http://www.lowersriskgroup.com/blog/2014/06/03/fraud-risk-prevention/> [Accessed 06.06.2015].
19. National Treasury (n.d) fraud prevention policy. <http://oag.treasury.gov.za/RMF/Pages/s204FraudPreventionPolicy.aspx> [Accessed 06.06.15].
20. Omar, N., & Bakar, K. M. A. (2012). Fraud prevention mechanisms of Malaysian government-linked companies: An assessment of existence and effectiveness. *Journal of Modern Accounting and Auditing*, 8 (1): 15-31.
21. PWC. (2013). Fraud risks for higher education institutions. <http://bufdg.ac.uk/ViewDocument.aspx?t=1&ID=2329&GUID=a434a94b-5fc5-4d82-b401-92b2c40fe92f&r=1> [Accessed 06.06.2015]
22. RACC (n.d). Become a certified professional research or sponsored programs administrator <http://www.cra-cert.org/> [Accessed 03.06.2015].
23. Rahman, R. A., & Anwar, I. S. K. (2014). Effectiveness of Fraud Prevention and Detection Techniques in Malaysian Islamic Banks. *Procedia-Social and Behavioural Sciences*, 145: 97-102.
24. Reja, R., Manfreda, K.L., Hlebec, V & Vehovar, V. (2003). Open-ended VS. Close-ended Questions in Web Questionnaires. *Development in Applied Statistics*. 160-177.
25. Richards, J. C. & Schmidt, R. (2002). Longman dictionary of language teaching and applied linguistics. Third Ed. London: Longman.
26. SABC. (2014). Fraud hampers funding at higher education. <http://www.sabc.co.za/news/a/Occa9f0042d0aa06bdeaff56d5ffbd92/Fraud-hampers-funding-at-higher-education-20140502> [Accessed 06.06.2015].
27. SAQA. n.d. Promoting genuine qualifications in Africa through effective verification. http://www.saqa.org.za/docs/news/2015/Post%20seminar%20article_v2%20final%20approved.pdf [Accessed 06.06.15].
28. Singleton, T.W. & Singleton, A.J. (2010). Fraud auditing and forensic accounting. 4th ed. John Wiley & Sons. Newrsey.
29. Sitorous, T.W. (2008). Fraud risk factors and auditing standards: an integrated identification of a fraud risk

- management model. Unpublished Master's thesis. Southern Cross University.
30. Taylor, J. (2011). *Forensic Accounting*. Pearson Education, Harlow.
31. Times Higher Education. (1995). <https://www.timeshighereducation.co.uk/news/grants-by-fraud-hit-institutions/95049.article> [Accessed 06.06.15].
32. Schwart, R., Larson, M & Kranacher, M_J. (2008). Helping to prevent university fraud. Deloitte Forensic Center.
33. Sitorous, T.W. (2008). Fraud risk factors and auditing standards: an integrated identification of a fraud risk management model. Unpublished Master's thesis. Southern Cross University.
34. Wilhelm, WK. (2004). The Fraud Management Lifecycle Theory: A Holistic Approach to Fraud Management. *Journal of Economic Crime Management*, 2(2):2-38.
35. Zohrabi, M. (2013). Mixed Method Research: Instruments, Validity, Reliability and Reporting Findings, *Theory and Practice in Language Studies*, 3 (2): 254-262.