Province of the
EASTERN CAPE
SOCIAL DEVELOPMENT

FRAUD PREVENTION STRATEGY/PLAN

EFFECTIVE FROM 01 APRIL 2017 TO 31 MARCH 2020

Province of the
EASTERN CAPE
SOCIAL DEVELOPMENT

Table of Contents

Executive Summary

It is important to define the aims of this strategy to ensure that those who are entrusted with the public funds are committed without fear to account for the funds allocated to their custody that they have been used solely for the purpose they were intended. The following is the aim of our robust counter - fraud strategy:

(a) Reducing fraud to an absolute minimum level
(b) Arrangements to manage and mitigate fraud at a minimum level, and
(c) Resources for better citizen's care, support, service delivery and reduction of poverty.

This document contains the strategies and action plans that the Department of Social Development (hereinafter referred to as the DSD) can implement to limit its exposure to fraud and corruption. The term fraud is used expansively, and is intended to include all aspects of economic crime and acts of dishonesty.

There are specific objectives to this strategy, which are generic in nature where this department must base their counter fraud work on and be committed to achieving it:

1) The creation of an anti fraud culture
2) The maximum deterrence of fraud
3) The successful prevention of fraud.
4) The prompt detection of fraud which cannot be prevented
5) The professional investigation of alleged fraud
6) Effective sanctions, including appropriate legal action against those committing fraud, irrespective of who they are
7) Effective methods of seeking redress in respect of money or assets defrauded.

Henceforth, it is Provincial Policy that no fraud against the Eastern Cape Administration will be tolerated, all **alleged** fraud and/or corruption will be investigated and all transgressors shall be punished both internally and externally to the fullest extent possible.

INTRODUCTION

The Public Finance Management Act, Act No.1 of 1999 (PFMA), as amended has its prime object to secure transparency, accountability and management of revenue, assets and liabilities of the institutions within a spirit of good governance, to which the act applies.

In South Africa, fraud is defined as:

"The unlawful and intentional making of a misrepresentation which causes actual prejudice or which is potentially prejudicial to another." – Criminal Law: Snyman Second Edition 504

Fraud in relation to DSD can be practical outlined as follows:-

"Improper, fraudulent, corrupt, irregular and immaterial access to resources for personal gain which could not have been achieved by proper means"

The above definition is practical and applicable to the Department of Social Development and it is without any limitations to other means and elements of fraud and corruption.

For the purposes of easy reference, the action plans are divided into the following 3 basic groups:

1. *The Fraud & Anti-corruption Policy*

Signing the policy and getting management buy in.
Staff sensitization and participation in fraud prevention.
The Reporting Officer, the National Fraud Hotline and rewards for whistleblowers.
Circulating the message to all staff members.
Internal and external publication.

2. *Managing Human Resources*

Staff Vetting.
The Code of Conduct for the Civil Service and a Departmental Code of Conduct and Ethics.
Registers of interests and gifts.
Fraudster blacklist register.

3. *Managing the Fraud Risk*

3.1 Fraud risk assessments and regular review of prevention and detection controls that are designed by management to mitigate fraud
3.2 Rating of position susceptible to fraud
3.3 Surprise audits and spot checks.
3.4 Supplier and trading partner awareness.
3.5 Fraud prevention training.
3.6 Assessment industrial and external fraud risks.

FRAUD RESPONSE PLAN

SECTION 1: THE FRAUD & ANTI-CORRUPTION POLICY

1.1. Fraud & Anti-corruption Policy Statement: Getting Management involved

The purpose of this document is to set the tone through which top management commit themselves and their entity towards rejecting fraud as a business norm. By publishing this "mission statement" the DSD irrevocably binds itself to combat all forms of fraud and corruption and binds the Department to remain proactive in the fight against fraud and other white-collar crime.

Inherent to the nature of their duties, it is the responsibility of Senior Management of the DSD to prevent fraud in the workplace. An integral part of the statutory and common law duties of Senior Management towards the State and the Public is to prevent fraud from seriously impacting on the delivery of services of the entity. This responsibility should be seen to be accepted and emphasised through the promulgation of the Fraud Prevention Policy by the Head of Department, acting on behalf of Senior Management. This document is aggressive and firm, covering *inter alia* a zero tolerance attitude towards fraud and corruption, an undertaking to aggressively seek it out, to investigate all allegations, to prosecute offenders, and to encourage staff to report any incidences. Extracts from this document should be distributed to all staff members and stakeholders.

The **Fraud & Anti-corruption Policy Document**, which will be signed by the Head of Department, sets the attitude towards the problem and declares a zero tolerance. The fraud policy statement contained in this document reads as follows:

"I, Stanley Khanyile, in my capacity as the Superintendent General of Department of the Eastern Cape Department of Social Development, wish to restate the ZERO TOLERANCE policy towards fraud and other acts of dishonesty. The Department's values include INTEGRITY and HONESTY. As a Department, it is important that we take these values seriously and ensure that we do not permit activities that are not aligned with our departmental norms and standards. It is incumbent on all of us to be intolerable of this behaviour and to report such findings. To this end, defrauding the Department will not be tolerated and those employees or other stakeholders found to be in violation of this policy will be prosecuted to the fullest extent possible, both internally and externally."

1.2. Staff sensitisation and participation in fraud prevention

The purpose of the Fraud Prevention Policy Brochure is to launch the fraud prevention strategy in the DSD and to introduce the zero tolerance principle to employees.

A document outlining the Department's attitude towards fraud is distributed to staff member via the Departmental Intranet and Internal Magazine. The Fraud Prevention Policy Brochure will be a document that is made available to all staff members and should be worded in such a way as to achieve "buy-in" from all staff. It should create a certain level of fraud awareness among staff members, encouraging them to detect and report fraud in the workplace.

This document covers aspects such as the need to have a policy, defining the various offences, setting out the reporting structures, assigning responsibility to designated officials, making provision for training, selling the hotline concept, publication, non-fraud irregularities, confidentiality, anonymity, protection of whistleblowers rights, etc.

1.3. The Reporting Officer, the National Fraud Hotline and rewards for whistleblowers

The purpose of the Reporting Officer and the National Fraud Hotline is to provide facilities through which all stakeholders can report suspected fraud or corruption in the Department. The Reporting Officer and the National Fraud Hotline are also useful tools through which the momentum and interest in the fraud prevention initiatives can be maintained.

Every organisation needs a channel through which employees, suppliers, contractors and other third parties can report irregular activities, free from victimization or other repercussions. For the DSD, there are two channels through which reporting may occur. The first is the Reporting Officer that will be appointed by the Superintendent-General of the Department for the purposes of receiving reports from employees and other stakeholders regarding possible fraud and corruption within the Department. The other is the National Fraud Hotline, created for the purpose of enabling civil servants and other persons to report fraud and corruption, safe from other repercussions.

The primary means of detecting fraud will and should always remain a sound system of internal controls and regular internal audits. These measures are, however supplemented with the Reporting Officer and the **National Fraud Hotline (0800701701),** a fraud-reporting channel where information regarding fraud is collected, and decisive corrective and preventative steps could be taken to limit the DSD's exposure to further or future loss. Vital to these functions is the assurance of anonymity, commitment to investigate all irregularities, protection of

the whistleblower and consistent application of the fraud policy, regardless of the seniority of the alleged offender.

Government has recognized the fact that the hotline concept has become an accepted business reality, which is recognised as a vital tool in fraud prevention. Various surveys have been undertaken on this subject over the years. All of these surveys have indicated that an increasing number of frauds were uncovered because of whistleblowing. These were either in the form of anonymous calls or notification by either staff or outsiders. It is estimated that at least 25% of frauds are uncovered in this manner.

Employees must be encouraged to utilize this facility if they are not comfortable with utilizing the Reporting Officer.

Employees are often afraid to interact directly with management. To overcome this, it has, in the past, proven effective to provide an independent forum to communicate information or suspicions about fraud and corruption.

In order to be effective at combating fraud and corruption the Reporting Officer should also have mechanisms through which employees may report fraud and corruption anonymously. It is therefore recommended that a DSD fraud mailbox be created.

In order for the above reporting mechanisms to produce the desired results the following criteria must be satisfied:

- The facilities should be well advertised;
- It must be available and accessible to all staff;
- The Reporting Officer must be, and seen to be, independent with regard to the performance of his duties;
- Anonymity must be assured, as well as for the reports received by the Reporting Officer;
- Protection against recrimination must be guaranteed; and
- The potential users must feel that the information provided by them will be investigated, regardless of the position of the accused or his or her standing in the organisation.

To be effective, the following processes must be maintained:

- Proper record of all information received must be kept;
- All information must be channeled to the Risk & Fraud Committee, where it should be dealt with in accordance with the fraud response plan;
- Should the information be useful and a fraud be uncovered as a result of it, proper action/steps must be taken against the perpetrator;

- Where applicable, a reward could be paid to the whistleblower. It is the prerogative of Top Management to decide on whether rewards will be awarded and what the nature thereof will be.
- Should the information be insufficient or should the outcome of the investigation be negative a proper note to that effect should be made and this should be placed on file.

Since it is unavoidable that information on non-fraud related matters would also be received, provision must be made for communicating such information to the relevant division. Such information should not automatically be ignored as it may result in the whistleblower losing faith in the system.

As a number of the calls received may be malicious, it is important to assess the credibility of the information before an extensive and expensive investigation is undertaken. In accordance with the response plan, a thorough and discreet preliminary investigation should reveal the true nature of the allegations.

The Chief Risk Officer ("hereafter then referred as Reporting Officer") and the National Fraud Hotline can only be successful if it is well marketed and if it reaches all the employees and other stakeholders who may have information which would be of interest to the Reporting Officer. Marketing of the hotline is therefore a key to its success.

Many innovative marketing approaches are available. Some of the marketing avenues are listed below:

- Posters placed in all strategic locations;
- Hotline business cards;
- Telephone stickers;
- Advertisements in newsletter;
- Notice board;
- Text insert on pay slip;
- Group SMS;
- Letter to suppliers and trading partners;
- Road shows;
- Insert on letterhead;
- Rubberstamp on envelopes for all outgoing mail, etc;
- Startup message on computer for staff; and
- Message flashing on intranet.

1.4. Circulating the message via Road Shows

The intention of the road show is to ensure that employees are informed of the Department's efforts as well as their own responsibilities to combat and

report fraud. It also creates an opportunity to provide relevant training to outlying areas thereby reaching a larger audience.

It is important that the concept of preventing fraud is embraced by all the employees and other stakeholders of the organisation and that the aims and objectives of the plan are "sold" to the staff. Effective marketing is therefore critical to the strategy's success. As an additional marketing opportunity, a road show has great potential benefits, especially at the initial implementation stage. This would further demonstrate management's commitment to the project to all employees.

In order to effectively introduce the Fraud Prevention Plan (hereinafter referred to as FPP) to accountable managers and supervisors within the Department, it is essential to perform fraud awareness where the elements and practical working of the FPP can be explained. All the offices and other sites of the Department should be visited in order to achieve this aim.

1.5. Internal and external publication

The purpose of providing feedback about successes in the fraud prevention initiatives of the Department is to keep all employees sensitised and informed about continuing efforts in this regard, maintaining interest in the FPP, and to provide for a regular forum through which related matters can be addressed and brought to all staff's attention.

Once the concept of fraud prevention has taken hold in the Department and all employees have embraced the concept, a page in the Department's newsletter is a very effective medium to propagate these principles. If a regular newsletter does not exist, it should be considered to introduce a monthly publication, dedicated to fraud prevention that will be administered by the Fraud Prevention Committee that will be utilized to communicate policies and successes. It can also be used as a training tool to alert all staff members to current risks and new exposures. This newsletter should also be used to publish details of punitive measures taken against transgressors, emphasising the principles of the fraud policy.

To maintain interest in the fraud hotline, a monthly or a regular summary can be published setting out some details of the calls received by the hotline and action taken. Any successes arising from the fraud hotline can be highlighted in this publication.

SECTION 2: MANAGING HUMAN RESOURCES

2.1.1. Staff Vetting, the first line of defense

The purpose of the staff vetting process is to ensure that the Department limits its vulnerability and exposure of hiring and keeping potential fraudsters and criminals by ensuring they are armed with all relevant details about the incumbents applying for, and occupying positions.

It is far easier not to employ a high-risk category individual than to get rid of a dishonest employee later. A major focus of the fraud prevention strategy should therefore be geared to being very proactive and selective of persons to be employed in the Department. Applicants should be screened before employment is offered.

Employee vetting is a vital element in selecting and placing the right person for the right job. There are no shortcuts to this process and the risks associated with mistakes made here are significant. Although essentially Human Resources' responsibility, the Fraud & Risk Committee should have an input with regard to all positions and specifically for certain critical risk positions. Their input should also be obtained if the vetting or referencing process indicates prior improprieties with regard to the incumbent.

The employee vetting process will typically include obtaining information with regard to the following aspects:

- Reference checking;
- Criminal records;
- Civil records;
- Disciplinary records;
- Insolvency;
- Other businesses, directorships, memberships;
- Qualifications; and
- Other facts contained in the CV (physical address, ID number etc).

2.1.1. Reference checking

When screening potential employees, thorough reference checking is vital. This is a process which is often neglected especially by placement agencies. It should never be assumed that a personnel agency has been thorough in their reference checking as they have a financial interest in the placement.

When checking references of prospective employees, care should be taken that the prospective employee's entire career history is disclosed. Gaps in employment are often disguised under the excuse of "working from home" or "tried my own business", etc., whereas in reality, that person may have been dismissed for dishonesty or serving a jail sentence.

Very few people who are dismissed for dishonesty will disclose this fact. They are more likely to state for example that they had "a disagreement with management". These statements must be treated with the greatest circumspect. Always consider the likelihood that a fraudster will continue to defraud until they are brought to book. They also are likely, if they have defrauded their previous employer, to defraud their new employer.

A person who was dismissed will also be very selective with regard to the references supplied. The value of reference checking is therefore limited. More positive results may be obtained by contacting the Human Resources Department of a previous employer of the incumbent.

The permission of the incumbent to obtain any information from previous employers should be obtained in writing before the vetting process is initiated.

The employee vetting process can only be considered as complete when the organisation has the absolute assurance that there were no undisclosed acts of dishonesty relating to previous employment.

2.1.2. Criminal records

It is important for the employer to know whether a prospective employee has a criminal record as this would significantly affect the risk profile. Differentiation should be drawn between crimes involving dishonesty and crimes that are not likely to affect the employee's work. It should therefore be a requirement that all applicants submit full disclosure of any criminal records. In addition, non-disclosure of a criminal record must be made a dismissible offence to which the applicant agrees from the onset, i.e. on the same form. Pending criminal cases must also be disclosed.

With the consent of the incumbent it is relatively easy to obtain records of previous criminal convictions.

2.1.3. Civil records

Civil records give a good indication of possible bad habits of incumbents. If a person is recruited for a management position, it is important to determine whether that person has any civil judgments or adverse reports. A prospective manager may prove to be unsuitable for the post if his or her credit history reveals major financial indiscretions in their past. As civil judgments affect the risk profile of an

individual, it is important to consider this factor before employment is confirmed. Civil judgments are easily obtained through any of the credit bureaus.

As with criminal records, all prospective candidates must be required to disclose any civil judgments against them. This should include pending civil matters. Failure to disclose this information should be regarded as a disciplinary offence.

2.1.4. Disciplinary records

It is important for the entity to know whether the candidate has a history of disciplinary actions against him from previous employers.

As with criminal cases certain disciplinary actions may be irrelevant from a fraud risk assessment perspective. All disciplinary actions by previous employers should be considered carefully. The permission of the incumbent to obtain disciplinary records should be obtained in writing.

If a person has been dismissed for dishonesty, it stands to reason that this authorisation referred to above will not be granted. In cases where authorisation is not granted the entity should increase its diligence in its reference checking process. Failure to permit the Department to check previous disciplinary records would also affect the risk profile of the incumbent.

It is easier to obtain detailed or sensitive information from an applicant than from an employee. The applicant seeks employment and is therefore at a disadvantage. The employee is already entrenched and can refuse to disclose information without fear of repercussions.

The disclosure of disciplinary action should include those that were settled.

2.1.5. Other business, directorships or memberships

It is important to ascertain from all applicants whether they have other businesses in which they are involved as an officer or hold a share. This information is important as it could impact on the applicant's objectivity if he or she would be in a position to favour that entity. In addition other businesses could affect the person's income and time available and may explain why an employee is maintaining a lifestyle above his or her known means.

At the application stage it should be a requirement for all applicants to disclose that information. The disclosure should then be compared to the results of the screening process, which could give an early indication of dishonesty. Anyone caught not disclosing other business interests should not be employed. In addition, it should be considered a disciplinary offence if dishonesty in this regard is discovered later.

A Companies & Intellectual Property Commission (CIPC) checks will give an indication of any directorships of companies or memberships of close corporations. It will of course not give any indication of any businesses conducted as sole proprietorships.

In addition, the employment contract should provide for immediate disclosure of any new interests / directorships once the person is in employment.

2.1.6. Qualifications

Most applicants will submit curriculum vitae in support of their application. This CV will typically list all academic qualifications. The entity is exposed if they appoint a person who has alleged qualifications that they did not obtain. Apart from the obvious operational risks, this is also an indication of a tendency of dishonesty.
Most fraudsters who submit false qualifications will focus on qualifications that are difficult to confirm, especially from foreign universities or universities that have subsequently closed etc. When vetting, such university qualifications should be considered as high risk.

Details regarding academic histories are readily available and not too expensive. Qualifications checks should be undertaken not only for applicants but also for current employees as part of the fraud prevention initiatives and employee risk assessments.

2.2. The Code of Conduct for the Civil Service and a Departmental Code of Conduct and Ethics and Code of Conduct for Social Service Professionals

A comprehensive Departmental Code of Conduct and Ethics is essential to ensure certainty amongst staff regarding the rules of the Department.

Fraud thrives in an environment devoid of morals and ethics. Therefore, at the heart of the cure lies the establishment of an environment that is rich in moral and ethical values and behaviour. The adoption of a well thought out Departmental Code of Conduct and Ethics, encompassing the highest level of moral and ethical values would be critical in ensuring the success of any fraud prevention strategy. The Departmental Code of Conduct and Ethics must be a separate document tailored and adapted to suit the DSD in respect of all its activities and not only fraud prevention.

The drafting of a Code of Conduct and Ethics that is aligned with the Government Code of Conduct is essential to the well-being of fraud prevention within the department.

2.3. Registers of interests and gifts and a fraudster blacklist

The purpose of the registers and the blacklist is to ensure that the Department is aware of interests of staff members in the affairs of the Department, the extent of entertainment and other benefits received by employees from suppliers and other business partners and to provide the Department with a record of previous problems with regard to suppliers.

2.3.1. Register and Declaration of interests

It is often found that employees take advantage of their position in an organisation to procure extra benefit for themselves by having an interest in suppliers or other business partners to the Department. In order to ensure the total objectivity of employees with regard to suppliers, it is necessary to keep a register of all interests that employees may have in other entities. It should be the duty of every employee to report his or her involvement of any nature, with another entity, to the Department. Directorships, shareholding, memberships and any other relationship with other entities should be disclosed. This should also include close family members. Keeping this register updated should also provide some insight into staff members that perform other work for remuneration that may have an influence on their performance for the Department. Reference to the Public Services Regulation of 2016 should be made all the times.

2.3.2. Remunerative work outside the Public Service

Every employee should obtain authority from the Executing Authority for all remunerative work outside the Public Service in terms of the Public Service Act, 1994, as amended and Public Service Regulation of 2016, as amended

2.3.3. Register of gifts and other benefits

Gifts and other benefits received from suppliers or other business partners of the Department should also be made reportable. Corporate entertainment and corporate gifts can lead to employees benefiting certain suppliers to the detriment of the employer. It can also lead to serious corruption and fraud. Making gifts and other benefits reportable creates the opportunity to establish trends and to identify a situation before it becomes a problem. The Departmental Code of Conduct and Ethics should make it a dismissible offence not to report gifts and benefits. This will enable the Department to discipline transgressors without having to prove a corruption case.

2.3.4. A Fraudster Blacklist

It happens often that entities that defraud government departments, and are caught out, merely change name and shape and return to government to continue their activities. A fraudster blacklist should be created that contain all the Department's suppliers' ID numbers, addresses and other available information pertaining to all individuals that were involved in an entity that defrauded the Department. This information should be readily available to employees of the Department and should be consulted before procurements are made from suppliers. All employees' particulars that were involved in such activities should also be recorded in the database for future reference. In this manner, a database of *persona non grata* is built up to assist the procurement managers in selecting suppliers. The database should be easily accessible to all managers at all the sites of the Department for ease of reference.

SECTION 3. MANAGING THE FRAUD RISK

3.1. Economic crime, Fraud Risk Assessments and Grading of Positions

3.1.1. GENERAL: EXPOSURE TO FRAUD AND OTHER ECONOMIC CRIME

The DSD is exposed to a vast number of different types of fraud, many of them generic to the public sector. Generally speaking, fraud can be categorised into employee fraud or management fraud. Both internal and external parties could defraud the Department.

We list a number of different categories of fraud that the Department has exposure to, which will serve as a checking list to management to assess the adequacy of their controls. The list and descriptions should also be used as a training tool for Forensic Auditors. See annexure A.

In this document, fraud is used as a generic term that includes all types of economic crime and related misconduct. It should be noted that the legal definition of fraud limits the terms as described below.

Economic crime is generally considered to be a crime of a non-violent nature, which involves actual or potential losses to rightful owners, usually by means of deceit or misrepresentation. The term includes, but is not limited to the following:

- Fraud;
- Theft;
- Computer crimes;
- Extortion;
- Corruption;

- Irregular money lending;
- Forgery and uttering; and
- Conflict of interest.

The Department is exposed to more than one type of economic crime at all levels and to varying degrees. Attached hereto as annexure A, is a chapter, detailing the various types of economic crime.

3.1.2. FRAUD RISK AND VULNERABILITY ASSESSMENTS

This section provides a guideline for assessing risk and fraud susceptibility in the Department, so as to proactively address possible pitfalls with regard to fraud and other economic crimes.

There will never be sufficient time to assess all functions or to evaluate all employees, officials and stakeholders to identify who are likely to defraud the DSD&SP. The fraud prevention team should therefore have procedures to identify high-risk areas and employees, officials and stakeholders within those sectors. The process has separate legs:

- Identify areas of exposure;
- Grade positions in the exposed areas in terms of risk exposure – low, medium, high, and critical;
- For all high and critical risk positions, employees and officials filling those positions should be subjected to a vetting procedure to determine whether they pose a fraud risk; and
- For all employees who appear to pose a fraud risk, due to their personal profiles and who are employed in high or critical risk positions, fraud testing should be conducted.

Identify areas of exposure

This is a logical process where the Fraud Prevention Committee assesses where the Department is exposed to fraud and what type of fraud. It may be any type of exposure i.e. cheque fraud, procurement fraud, computer fraud, etc. This assessment should be based on current trends within the public sector, or on rumours and allegations, or be triggered by discovery of similar frauds at other venues. The assessment of fraud exposure per type and per venue should be linked to a monetary value to facilitate a prioritisation process.

The assessment should involve local management of each division, by requiring them to complete a self-assessment in terms of their risk profile. If this approach is adopted, it has the added benefit of forcing local management to at least consider their own risk profile, which is beneficial to their day-to-day management. The process can be used in a top-down or pyramid fashion where the local head requires all heads of departments to complete this form, who in

turn will send it further down to heads of sections, etc. Through this process, most members of management (at all levels) will develop greater fraud awareness, and everyone will recognise the proactive steps taken by the management to restrict the Departments fraud exposure, as set out in the fraud policy.

This process highlights the need to approach fraud jointly, by asking everyone to contribute to the fight as opposed to a "**them** versus **us**" attitude.

The result of this assessment should be collated by the fraud prevention team for a detailed prioritisation and planning process.

Rating positions in the exposed areas

In the identified areas of exposure, a further assessment is required to determine whether any fraud has occurred, or whether it is possible that a fraud may be in progress. This is a very subjective test and should be used as a guideline for prioritisation purposes only.

If the first exercise has revealed an exposure to the particular type of fraud, the Fraud & Risk Committee must further assess which positions are most exposed and where the heaviest reliance is placed. For this purpose, consider the adequacy of all internal controls. A problem of segregation of duties in this particular section should always be given priority. As a starting point for this exercise, all control issues raised by external and internal auditors over the previous years will provide guidance e.g. if procurement fraud has been identified as a major risk, the procurement officer's job functions must be assessed to determine that officer's ability to defraud. If the historical audit reports have identified controls in this sector as deficient, a high-risk classification is justified. The risk classifications should be considered as either low, medium, high or critical.

Low risk implies that the internal controls are very good, the segregation of duties is more than adequate and the supervisory and custodial controls are effective. In addition, there should be no known or rumoured losses in that section.

Medium risk for the position implies good internal controls, adequate segregation of duties and good supervision. There should be no audit queries relating to controls issues emanating from that position. There should be an assessment that there is heavy reliance on trust, but that it does not appear to be a problem.

High-risk areas are the positions in sectors which are potentially exposed. Controls will be deficient, heavy reliance will be placed on trust, supervision is inadequate and there are historical audit queries. In addition there may be historical losses (i.e. stock shortages, etc).

Critical risk positions imply all of the factors considered under high risk above, but coupled with known shortages and a position where the incumbent can do considerable damage to the DSD.

This section should only be prioritised for those sectors where there is a perceived exposure to fraud as opposed to all sections.

Grade employees

For the high and the critical position grading assessment, it is a priority in terms of fraud management to assess employees who hold those positions. This is an objective process and will be guided by the information gathered with regard to the particular person. In addition all the factors about identifying potential fraudsters discussed above and below should be considered.

The employees should be graded as low, medium, high or red, based on the results of this and other reviews.

Low and medium risk employees are those who do no not fit into the profile of the fraudster and there have been no suggestions to the contrary. It is dangerous, however, to classify employees too hastily into low or medium risk, as it is part of the profile of a fraudster to appear to be above suspicion.

High-risk employees are those who fit the profile according to the vetting done on them. The vetting is similar to the vetting that is done on a staff member when he is employed by the Department as discussed above in paragraph 2.1.

Red risk employees are those who not only fit the profile, but there are actual fraud alerts. These can include anonymous tip-offs about the employee, a track record of indiscretions, repeated warnings, those who got off on a technicality previously, those who have prior criminal records, those who have been dismissed for dishonesty from previous positions or offices held, etc.

Typically the assessment for a red risk employee who is placed in a high or critical risk position should suggest a perception of "we know he is stealing but have not caught him yet". Such an employee should be "profiled" in the manner suggested later in this document.

Test for fraud

Proactive fraud auditing is justified for all sectors which are exposed to any type of fraud, where the positions have high or critical grading on which are filled by high or red risk category employees. The testing for fraud is very open ended and requires a number of complementary skills. Some guidelines are given in Annexure B attached hereto. If fraud is discovered, the elements contained in the fraud response plan should be followed.

3.2. Surprise Audits

The purpose of surprise audits is to provide a proactive forum to uncover fraud, to provide a deterrent to potential fraudsters, and also a reactive measure which can be used at the commencement of a new investigation to gather and safeguard evidence.

The concept of surprise audits can be a major deterrent to fraudsters as auditors could visit them at any time. External audits are planned well in advance and are usually anticipated by all staff. The same holds true, but to a lesser extent of internal audits. As all or most affected staff members know, or can anticipate the timing of these visits, the element of surprise is lost. Fraudsters too are aware of these visits and have ample time to conceal their activities. They can hide (or misfile) or even destroy incriminating documentation in good time, thereby minimising the risk of discovery by auditors.

To be effective, however, the surprise audit team must maintain the following criteria:

- Maintain absolute secrecy;
- Be unpredictable;
- Be ruthless in application;
- Be multidisciplinary;
- Comprise of experienced team members;
- Obtain support from management;
- Have an open mandate; and
- Be flexible in their approach to assignments.

In essence, a surprise audit would be planned in great detail for locations that have been identified as high risk, or maintaining a fraud friendly environment. The audit my be undertaken either during office hours or after hours, on working days or weekends, and also with or without the employees being present.

Advantages of having the staff members present include the possibility of assessing their reactions to the audit and/or the detailed scrutiny of documents under their control. Other advantages include the possibility of interviewing staff on suspicious matters or other issues, which require an explanation. Having staff present also minimises the risk of allegations of personal possessions disappearing.
Advantages of staff being absent during the audit include the unhindered scrutiny of all relevant files and documents by the audit team, as well as unhindered access to work areas.

Disadvantages of a surprise fraud audit in the absence of the staff members are the restrictions imposed on the audit team, as they now have to focus almost exclusively on documentary evidence. If the staff members are present, the team could also assess any behavioral peculiarities displayed by certain staff members under the pressure of the occasion. A major disadvantage to keep in mind when planning a surprise audit "in absentia" is the disruptive effect on normal operations.

The decision on how to undertake the surprise audit should be based on an assessment of all the above factors. A combination of approaches may prove most beneficial. A combination may, for example, entail commencing a surprise audit of an institution or corporate service center, on a Friday afternoon (with staff present), and continuing into the night and over the weekend. This approach would achieve most objectives, whilst negating certain disadvantages, noted in respect of employee presence and absence.

Every high-risk environment should be audited at varying degrees. In the principle office, a **surprise audit** at least twice a year must be conducted even if it is in quick succession. (Speed traps positioned close to another are likely to catch more speedsters as the latter are under the impression that they have escaped the trap and drop their guard.) This approach could further act as a major deterrent or prove highly successful at uncovering fraud.

The constitutional rights of employees must, however, be respected. If auditors or investigators, in their zeal disregard an employee's right to privacy, any evidence they obtain could be rendered useless or inadmissible. A fine balance must thus be maintained between the Departments right to safeguard their assets and the employee's right to privacy.

3.3. Procurement procedures and supplier and trading partner awareness

The purpose of this section is two fold, that is, firstly to obtain all relevant information about the DSD's trading partners to limit their exposure to unsavory business associates and secondly, to incorporate these trading partners into the DSD's fraud limitation and prevention initiatives.

The Department, due to the magnitude of its operations is significantly exposed to procurement fraud. To minimise the risk several initiatives may bear fruit:

- Get to know your supplier;
- Set the ground rules;
- Set a clear guideline on "unacceptable gifts"; and
- Report extortion to the Fraud Prevention Committee.

There are several legs to this approach:

- Commit employees and suppliers to a procurement procedure;
- Ensure that the Department knows exactly with whom they are dealing. This can be achieved by asking for all relevant information directly from the supplier.
- Encourage trading partners to become actively involved in fraud prevention and early reporting.

3.3.1. Procurement procedure

Just as the Department binds its employees to abide to the entity's Code of Conduct and Ethics, they should be bound to a procurement procedure designed to eliminate the risks of procurement fraud. Suppliers and trading partners should also be subjected to this procedure. This document should endeavour to provide for policies and procedures, designed to eliminate subjectivity from the selection of vendors and promote transparent and fair procurement.

3.3.2. Know your supplier

As part of the DSD's fraud prevention strategy, all vendors are required to actively assist in eradicating fraud and corruption from the organisation.

Vendors and suppliers are required to register to the approved supplier list (CSD).The systems is managed by the Treasury. Suppliers are required to visit the provincial treasury's website to register online (www.treasury.gov.za). DSD will not do any business with a supplier that is not registered on the Central Supplier Database.

This information is required for all enterprises supplying goods and services to the DSD as well as those tendering or quoting for work.

Information required will typically be:

- Trading Name of business partner;
- Full details of business entity;
- Registration number;
- Year in which business commenced;
- Physical address;
- Postal address;
- Telephone number;
- Fax number;
- Cell phone number of manager;
- Directors / Members (id numbers required);
- Manager of office / branch;

- Goods or services supplied to the DSD (nature);
- Principal shareholders;
- VAT and income tax number of enterprise; and
- Bank account details (for direct deposits).

Any information supplied by the supplier during the registration in the CSD and turns to be incorrect may easily be used against the supplier to lay fraud charges as the supplier submitted misleading information.

Documentation required

- Registration documents (Companies and Close Corporations);
- Tax clearance certificate (for all companies supplying goods or rendering services valued in excess of a large amount, for example, R1 m per annum.); and
- Municipal and rates clearance certificates

Reporting of fraud and corruption

The supplier or trading partner should also be informed in writing of the following:

Any incident where a department employee attempts to solicit favours, gifts, kickbacks or donations from suppliers or vendors must be reported forthwith to the Risk & Fraud Committee. Under no circumstances may the supplier or vendor concede to any such requests or demands from any employee, unless so instructed by an investigator, duly appointed by the Head of Department.

Any evidence of fraudulent activity must be reported to the Risk & Fraud Committee or Provincial Treasury

3.4. Training for staff members and management

The purpose of the comprehensive training program is to highlight the risk of fraud and corruption in the Department, empower employees to recognise it in its infancy and to guide the fraud prevention team in the most optimum processes in combating fraud.

Training is vital component for the success of every fraud prevention program, as this is the process through which the employees are empowered to become actively involved in fraud prevention and detection. A number of modules are available and should be presented at varying levels, depending on staff category and their future role in the process.

More intensive training should be presented to management, whose duty it is to prevent and combat fraud.

All other staff members will be reached through the presentations referred to above under "road shows"

The training can take the form of lectures, presentations, seminars, self-study and workshops. To be effective however, training must be followed up at least on an annual basis.

Refer to Annexure C attached hereto for broader illustration.

ANNEXURE A

FRAUD

Fraud is described as an intentional misrepresentation, which results in actual or potential prejudice. This is a very wide description and covers many different forms of fraud. Department is exposed to inter alia:

- Procurement fraud;
- Employee fraud;
- Management fraud;
- Computer fraud;
- Electronic Banking Fraud;
- Stock fraud;
- Time fraud; and
- Manipulation of records and documents.

Procurement Fraud

With the Department's massive purchasing power, it has to make significant purchases. Through this process it is exposed to procurement fraud, i.e. fraud relating to the purchasing of goods or services. This can take the following forms:

Cover quoting	Obtaining multiple quotations at inflated prices from linked organizations and process Orders and GRVs in record time.
False invoices	Over invoicing, non-delivery of goods purchased, and false instructions to other officials to capture GRVs etc.
Under supply of	Paying for more items or services than delivered or

goods or services	rendered or submission of same invoices more than once for same services.
Corruption / kickbacks	A "sweetener" given to the procurement official to favour the giver. This can ultimately, if unchecked, develop into extortion where contracts are not awarded without financial kickbacks to individuals in the buying office.
Inferior products at inflated prices	Paying premium prices for inferior goods or sub-standard services.
Trademark infringements	Paying actual prices for counterfeit goods.
"Own companies"	Managers may place orders from companies they own, or in which they have a financial interest or have sole signing powers in such company's bank accounts
Nepotism	Although not a crime, there is a risk that a friend or family member may be awarded lucrative contracts, which could be at the expense of the entity.
Double payment	Duplicate payments for the same goods and services, including erroneous 3rd and 4th Tranche Payments to NGOs.
False specifications	Intentionally setting false or irrelevant specifications to eliminate potential suppliers and unduly favouring other specific suppliers.

In the above-mentioned cases the threat is internal and external. Officials may facilitate the crime either for a share in the profits or for kickbacks. The bigger the group, the higher the risk that these may go undetected. With internal involvement, it is difficult to identify, as paper work may be destroyed or altered after the event. In addition, other internal controls may be compromised or bypassed. Stock counts and reconciliation can be amended to conceal shortages. The differences may be written off in the books to further conceal shortages. This threat is not unique to any operation of the Department or to the country.

Employee Fraud (payroll fraud)

With a massive workforce, the Department is exposed to a wide variety of employee fraud. For these purposes we focus only on frauds associated with the labour function. Employee fraud, per definition is much wider but covers all other frauds conducted by employees.

The employee frauds, discussed briefly below, are internal threats, except where the entity makes use of external personnel agencies, in which case the threat is both internal and external.
These threats are not limited to any particular business entity and are universal..

Ghost workers	Fictitious employees on the payroll.
False qualifications	Employees employed on strength of false qualifications. Submission of false documents to gain employment.
Unauthorised increases, promotions and bonuses	Employees processing unauthorised master file amendments resulting in overpayments.
Kickbacks	Employees defrauding the group for share of illicit gains. Any employee receiving kickbacks could have undertaken action to the prejudice of the group.
Nepotism	Although not a crime, staff members employing their own family members may compromise the company.
Falsification of leave records	Unauthorised amendments to leave records will prejudice the entity, especially when the employee leaves the service of the entity and is paid out more than due. The same counts for not submitting leave forms for leave taken, i.e. inflating leave due. This, if in collusion with management, can result in significant losses.
Subsistence and travel claims fraud	False, duplicated or inflated claims.
Personnel file manipulation	Unauthorised manipulation of the personnel files can pose a risk. Disciplinary records can be deleted exposing the group to risk if these employees are promoted to more senior positions.

False deductions	Staff in the personnel section may process unauthorised deduction from the permanent staff's salaries, redirecting these deductions into accounts in which they have an interest.
Timesheet / clock-card fraud	Processing and being paid out for work not done or clocking other employees' clock cards will result in a loss.
Conducting private business during office hours	Management and staff conducting private business during office hours steal time from the entity.
Unauthorised use of Departmental resources for private purposes	The Department is exposed to management and staff abuse of Departmental resources for private purposes. This can include use of assets or personnel.
Improper hiring procedures	With employees employed in sensitive positions, possible at management level or in a position requiring the handling of cash, it is vital that proper reference checks are made. Failure could result in expensive and embarrassing situations for the Department.
Cover Quoting and Anti-Competitive Bidding	Inflation of quotations and manipulation of maximum and minimum prices in order to award fair advantage to a particular service provider over others.
Procurement fraud – Ghost Suppliers	Fictitious procurement of goods and services for ghost suppliers with ghost contact details and ghost goods. Procurement after hours and awarding of contracts to same supplier – double dipping.
Ghost Payments	Confirmation and Capturing of Goods Received Voucher without proper verification of rendition of services

The most effective protection against employee fraud is to have an honest and effective personnel section, carefully screened staff, regular review of staff,

proper disciplinary procedures, tough attitude to offenders, prosecute fully for theft, hire carefully, fire ruthlessly when appropriate, screen employees before placing them in sensitive positions, give management performance bonuses, led by example, encourage and reward good service, pay well and listen to grievances.

Contractors and suppliers should be screened with the same care as senior management.

Management Fraud

Management fraud is a wide term describing frauds conducted by management. By virtue of their position of trust, their better knowledge of the systems and internal controls, management override of internal controls, their access to more functions, as well as their ability to intimidate others, the Department is financially more exposed to greater losses at the hands of management than it is at the hands of other employees.

This is an internal threat, but is universal in that all entities, both public and private, in all countries are exposed thereto.

Computer and Systems Fraud

Computer fraud, as opposed to computer crime, is in essence a fraud in which computers are used. It could overlap with any other fraud. Typical examples could be processing false payments, amending stock records, inflating salaries, etc. Every entity using a computer is exposed to this fraud.

Other forms of computer fraud to which departments are exposed includes the intentional planting of viruses, hacking, unauthorised changes to programs and/or data as well as unauthorised access through password abuse. Computer crime is elaborated upon below.

Electronic Banking Fraud

If the Department makes use of electronic banking, it is exposed to abuse of the system. Using electronic banking means funds can be transferred to incorrect accounts, false accounts can be loaded, unauthorised withdrawals can be made, etc. The exposure is internal where management is involved, and external when other parties gain unauthorised access to siphon off funds.

Theft

Every organization that has goods or deals with stock or cash is exposed to theft by staff. This is a universal threat. Where custodial controls are inadequate, theft will occur.

Computer crime

As many of the computers are on line through networks, it is possible to gain access thereto by hacking. Hacking is a computer crime by which unauthorised access is gained into the computer by an outsider through the modem of the network. The hacker can use this method to alter the programs, to gain access to financial or other information, to plant computer viruses, etc.

It is vital that the Department protect itself against the advances of a hacker or computer criminal. This would include firewall protection, an up-to-date virus detection capability, above average password protection, data encryption, etc.

The threat of hacking is not only external. It can be facilitated by insiders.

Unauthorised access by insiders is a very real threat in the organization and poses an even bigger threat than outsiders hacking in. Just as the hacker can gain access, an internal party may also be able to infiltrate the security and cause havoc or significant loss.

Insiders getting in through the so called "back door" can now get access to change files they previously only had "read only" access to. They can change their salary, days leave available, period employed, etc. Furthermore they can channel payments to bank accounts controlled by them.

Every organization, which has a computer, especially through a network of live computers, is susceptible to computer crime.

Every Department which utilises computers should have a master policy defining access/security management and back-ups. Then rectify relevance of the use of the word organization/department visa-vis direct interpretation.

Extortion

Extortion occurs where a corrupt society has taken hold. It is the inverse of corruption, viz. where an official is offered an inducement to either not perform required duties or to perform irregular duties. Extortion entails requesting or demanding personal gratification for performing set duties. In large procurement offices there is a risk that contracts will be "bought" from officials once extortion takes hold.

The crime of extortion is committed when a person unlawfully and intentionally obtains some advantage which is not due to him/her from another by subjecting the latter to pressure which induces him/her to hand over the advantage.

Corruption

Corruption can be defined as the offering, giving, soliciting or acceptance of an inducement or reward that may improperly influence the action of any person. It is therefore the act of giving or receiving reward (or offering or requesting reward) to an individual that is not due, to perform an action that he should not have, or not to undertake an action which he should have.

Corruption is a two-sided offence. The corruptor commits corruption when he/she corruptly gives, offers or agrees to give any benefit of whatever nature that is not legally due to another person to influence him/her to do his/her duty or to influence him/her not to do his/her duty (in other words to turn a blind eye).

The corruptee commits corruption when he/she receives, or agrees to receive or attempt to obtain any benefit that is not legally due either for himself/herself or for someone else to do his/her duty or to neglect his/her duty. (Examples of corruption: Offers to speed up processing of transactions on BAS/Persal/Supply chain management and not issuing a traffic fine)

Forgery and uttering

Forgery entails the falsification of a document, whereas uttering refers to its presentation. The Department is exposed in a number of areas, especially personnel, through falsification of curriculum vitae, qualifications, etc.

Forgery is committed by the making of a false document with intent to defraud, to the actual or potential prejudice of another.

The crime of uttering of a false document is committed when a person offers, passes off or communicates a forged document with the intent to defraud, to the actual or potential prejudice of another.

Both forgery and uttering are merely species of fraud. If a document merely contains false statements, it is not regarded as forgery and consequently the communication of the document cannot necessarily be regarded as uttering. A document is false when it purports to be something other than it is. This is the case when it is a spurious imitation of another document, or it falsely purports to be drawn up by a person other than its author, or to contain information that it did not originally contain.

The falsification can be achieved in many ways, for example by the alteration, erasure, substitution or addition of particulars on the document etc.

Conflict of interests

In conflict of interest situations the Department is invariably prejudiced. All employees must declare interest in contracts and potential conflict of interest situations. The appropriate registers, as required by the FPP, must be maintained and subjected to regular audit review. Failure to declare interest in other entities with whom the Department deals should be seen in a very serious light.

Counterfeit money, credit cards, cheques etc.

All outlets are exposed to the threat of counterfeit money, credit cards and cheques. Adequate precautions must be in place to protect these outlets.

Failure to report fraud and other irregularities

The failure to report irregularities or fraud that comes to the attention of staff members will result in disciplinary action against them. There are also statutory duties to report fraud contained in the Public Finance Management Act and the Prevention of Corrupt Activities Act that employees should take cognizance of. This principle applies both vertically and horizontally. It is therefore not only managers that are responsible to report the offences of their staff members, but the duty of every single employee to report irregularities and fraud of all their colleagues and other stakeholders, regardless of seniority or rank.

Suspicious documentation (procurement)

Unlike other crimes, especially those of a violent nature, fraud leaves no clear trails. There are many situations where it is not clear that a crime has been committed. The fraud will normally only be proven by the evidence contained in the documents.

The documents can however identify the crime before any other factors are known. Employees should be alert and familiar with red flags in order to identify suspicious documentation timeously. There are a number of factors, which should arouse the suspicions of employees. These are discussed below:

Invoices

Assess the following information and its appropriateness in the context it is submitted:

Type of invoice used, i.e. preprinted, accounting package, homemade or "CNA/Croxley";
Compliance with the VAT Act (must register if turnover is more than R300 000);
VAT registration number (10 digit number, must start with 4, fourth and fifth digit must read "01", etc.);
VAT charged at wrong percentage;

Date discrepancies (no date, date does not exist, postdated, pre-dated, date changed, etc.);
Address (no physical address, postal address does not make sense, etc.);
Telephone number (only cell phone number given, telephone and fax number the same, address and fax number in different regions, etc.);
Invoice number peculiarities (too high, too low, sequence intact, multiple sequences in use, numbers duplicated, do not run chronologically, etc.);
Business entity (public entity, private entity, close corporation, Section 21 entity, Incorporated, partnership, sole proprietor) unusual for type of product or service;
Registration numbers of entity (absent, inconsistent, irregular);
Clichéd or kitschy icons on letterheads (amateurish or inappropriate for business);
Trading name (very similar to other well-known companies, etc.);
Product descriptions (vague, impossible to assess);
Product codes (absent, inconsistent, etc.);
Inappropriate supplier for specific products (e.g. Caterer supplying vehicles);
Prices (unreasonable, impossible to assess, ridiculous, too cheap, etc.);
Round numbers (R10 000 for cables);
Guarantee (no reference to, not honored, multiple repeat invoices for services/repairs);
Handwriting (some written some typed, same handwriting - different entities invoices, familiar handwriting, etc.);
Presentation (original, original copy, photocopy, fax, photocopy of fax (header cut off), etc.);
Arithmetical inaccuracy (does not add up);
Signature (not signed, illegible squiggle, inconsistent, etc.);
Alterations made (tipex used, quantities changed, values amended, pencil entries, etc.); and
Reference to other "missing" documents (as per quote, as per list). Look for staple holes or paperclip indents, etc.).
Other documents

Consider other factors:

Use of photocopies
Multiple alterations
Different pens – same author
Missing documents ("The auditors have it")
Intentional misfiling
Departmental records kept at home

Documents found to be suspicious should be treated with utmost respect as they contain evidence of possible crime

ANNEXURE B

Fraud risk assessment – "high" and "red" risk category employee

To aid any prospective investigation, or to do preliminary testing to determine whether an investigation is justified, it is helpful to prepare a detailed profile on an employee who falls into the high-risk category. This profile should include the information as set out below:

Personal profile:

All personal details

Name, address, postal address, telephone number, cell phone number, office phone extension, salary level, deductions, bank account details, family members (include full names and date of birth of wife and children, wife's maiden name (if applicable), marital status, etc.)

Previous employment

Entity and position, duration of employment, salary level, reason for leaving and name of immediate supervisor.
If last employment was less than five years, repeat exercise for all previous employers, ensuring that the full employment period is covered. Do not restrict enquiries from previous employers to references given by the incumbent.
Determine (discretely or indirectly) whether there were any suggestions of impropriety with any previous employment

Personal habits

Record suspicions of gambling (horseracing or casino), excessive lottery ticket purchases, etc.

Background checking

Perform extensive background checking - record credit rating, directorships of other companies (own, wife, father, father-in-law, brothers, etc.), motor vehicles owned (own and immediate family), properties held (link to bond), civil judgments, adverse reports, RD cheques, etc.
Note which other companies have done background checks, recording details. Assess reasonableness of other enquiries. Contact such companies if necessary.

Qualifications

Confirm that qualifications submitted by the incumbent are legitimate.

Financial profile

Record remuneration levels as well as "take home" pay. Record whether the employee has other legitimate income from the office, i.e. reimbursed travel claims, subsistence allowances, etc. Ascertain whether the spouse is employed and if so, as what. Estimate a reasonable income level for spouse. Consolidate family earnings as "basic amount".

Behavioural profile

Record work profile in terms of leave taken, excessive accumulation of leave, excessive overtime, reporting for work even if sick.
Record observations of work – closed doors, secretiveness, nervousness if auditors are present, possessiveness about certain aspects of work, refusal of promotions.
Record peculiarities about behaviour patterns at work, emphasizing changes in trends, i.e. weight loss/gain, excessive sweating, irritability, inconsistent, mood swings, nervousness, unusual aggression, evidence of heavy drinking.
Record whether incumbent takes added initiative to learn about other employees' roles and functions, if so, which positions. Look out for added "experimentation" on computers and failed log on attempts under other staff's access profiles.

Access

Record to which sections, departments or offices the incumbent has access, either physically or electronically. Assess risk of other employees' computer passwords being used. Test to determine whether other employees' passwords were accessed from his/her computer and record full details.

Asset tracing

Perform low level asset tracing exercise

Work profile (for purposes of this exercise apply to a procurement officer):

Links to suppliers:

Assess whether the incumbent has a special relationship with any suppliers.

Consider known social contact, (invitation to parties, regular lunches, attendance at sport functions, joint holidays);frequent telephone contact between parties, use of private cell phone when phoning supplier, after hours telephone contact with supplier (test over leave period and from home telephone if possible);regular visits from/to supplier, closed doors when supplier visits, supplier conspicuous by absence (suggestion of secrecy in relationship);protective towards supplier's reputation; jobs (bursaries) for family; possessiveness in handling account; preferential treatment, (contracts and payment), unusually fast payments, quotes handed in after order date; deviation from normal procurement procedures (for this supplier only);one telephone call equals three quotes; and quotations and invoices hand delivered (procurement hands quotations and invoices to accountant), collects cheques on behalf of supplier or officer phones supplier to say cheques are ready, very frequent repeat orders, guarantees not claimed.

Province of the
EASTERN CAPE
SOCIAL DEVELOPMENT

ANNEXURE C

Training

Purpose:

The purpose of this training material is to give a better understanding of the whole concept of fraud and fraud investigation. It serves as self-study material to the Risk & Fraud Committee and guides on further initiatives that will aid early fraud detection and investigation.

Introduction

Although fraud will never be totally eliminated, it can be managed. There is no such thing as a small fraud. There are big frauds and there are frauds discovered when still small. If a fraudster is not caught perpetrating a small fraud, he / she will, in time, progress to committing big frauds.

The fraud prevention strategy is designed to help you to manage fraud. By managing fraud, you save money, reputation, effort and other limited resources.

The Department seeks to train those who will be actively involved in fraud prevention. It is not intended to be prescriptive, but to empower its users with an understanding of the principles of proactive fraud prevention rather than the reactive actual investigation of specific acts of fraud.

A prevention strategy paves the way towards good governance, greater transparency, improved morale and staff relations, and greater profits. To be effective, it requires the total and unreserved support of all - management and staff. It is a multidisciplinary approach that requires active participation of all sectors, namely, financial, operational, and marketing, human resources, trade unions, etc. To be effective the strategy has to be "sold to", and accepted by all.

Fraud management, however, requires more than lip service. There must be a clear acceptance of management responsibility. In addition, the infrastructure or capacity to investigate fraud must exist. The team must be empowered and an adequate budget provided for. Fraud management is expensive, but the rewards are substantial. If maximised, and if sufficient provision is made for the preventative aspect of fraud management, a savings ratio of 10 times the "investment" may be achieved.

Province of the
EASTERN CAPE
SOCIAL DEVELOPMENT

Fraud prevention initiatives require effective internal controls, a clear policy on the entity's attitude towards dishonesty, effective internal audit capacity, a strong investigative capacity and a track record of dealing harshly with transgressors – all known to members of the organization. As key players in the proactive prevention process, internal auditors, fraud auditors and investigators should focus on addressing factors that contribute to a "fraud friendly" environment and work towards eliminating these. In addition, in the course of their duties all role-players must develop an intimate "feel" for fraud alerts so that the frauds that do occur can be identified early and "nipped in the bud".

In the process of managing fraud, it is vital to understand the concept of fraud. Understanding, however, is wider than reciting its definition. It involves understanding how it is done, learning to identify "red flags", recognising the behaviour patterns of fraudsters and, very importantly, also understanding why it happens.

To eliminate fraud, either the opportunity to defraud must be greatly reduced, or the chance of early detection must be large enough and the action taken sufficiently aggressive, to make fraud an unattractive option to all stakeholders. If employees are convinced that they will be caught at an early stage and that the repercussions for themselves are going to be devastating, both professionally and personally, few will be tempted. By acting promptly, clear messages are sent to staff that the organization is not a soft target and will uncover all fraud, to the detriment of the fraudster.

The existing strategy approved in 2016/2017 financial year is expanded into a formal plan and further reviewed to be effective for period of three (03) years as from 01 April 2017 until 31 March 2020

COMPILED BY:

27.03.2017

MR. L.B. ZENZILE **DATE**
DIRECTOR – RISK MANAGEMENT & ANTI-CORRUPTION

APPROVED BY:

07/04/2017

S. KHANYILE **DATE**
SUPERINTENDENT- GENERAL