FRAUD PREVENTION AND ETHICS MANAGEMENT QUARTER FOUR PROGRESS REPORT 2020/21 FINANCIAL YEAR

Contents

1. BACKGROUND

In terms of the Public Finance Management Act (Act 1 of 1999), as amended, read in conjunction with Treasury Regulation, Public Service Regulation 2016, states that risk management and fraud prevention is a mandatory governance practice. Public institutions are required to have an approved risk management policy, strategy and plan which must include anti-corruption and fraud prevention policy, supported by an appropriated risk management system and architecture. It also states that the Accounting Officer should put structures in place to promote and educate the stakeholders about the department culture on fraud and corruption. Risk Management Unit is tasked with the responsibility of fraud and corruption prevention which include training of employees, fraud risk management and awareness. Risk Management Committee provides an oversight to the implementation of anti-fraud and corruption programmes.

The 2013 COSO Framework, the PFMA and the ERM Framework, are intended to be complementary. Fraud risk can affect areas beyond accounting and financial management activities. An organization seeking to minimize the adverse impacts of fraud needs to consider fraud risk in all areas of the enterprise and its operations.

2. EXECUTIVE SUMMARY

The department has established and communicated a Fraud Risk Management System that demonstrates the expectations of the senior management and their commitment to high integrity and ethical values regarding managing fraud risk. A fraud risk assessment process was conducted for identifying and assessing fraud risks relevant to the department. The fraud risk assessment addresses the possible risks of fraudulent financial reporting, fraudulent non-financial reporting, illegal acts and or corruption.

As a department we will strive to build and enhance our risk management capabilities that will better position the department on fulfilling its mandate and achieving its objectives. We reiterate that the responsibility and accountability for fraud and risk

management resides at all levels within the department and with each and every employee of our department.

In terms of the fraud risk monitoring, the report focuses on the top 18 fraud risks that will be monitored for the current financial year. There are several fraud risk mitigation actions that cut across different fraud risks.

3. PURPOSE

To report on the high risk areas of fraud and corruption, as well as to provide transparency of fraud risk areas that might possibly affect the promotion of good ethics and zero fraud tolerance within DWYPD.

4. FRAUD RISK AND ETHICS MANAGEMENT PROCESS APPROACH

The role of the risk management unit is to assist the department in the assessment and prevention of fraud risk and recommend risk action plans for managing them to protect the interest of the department and to promote ethics and anti-corruption. Governance structures including Audit and Risk Committees perform oversight over the activities of fraud risk and ethics management. The risk management framework governs the various risk areas including strategic, operational and fraud risk. This report outlines the fraud risk and ethics management progress made in the fourth quarter of 2020/21 financial year.

The Office of risk management performed a comprehensive fraud risk assessments to identify specific fraud schemes and risks, assess their likelihood and significance, evaluate existing fraud control activities, and risk implement actions to mitigate residual fraud risks.

A fraud control activity is an action established through policies and procedures that helps ensure that management's directives to mitigate fraud risks are carried out. A fraud control activity is a specific procedure or process intended either to prevent fraud from occurring or to detect fraud quickly in the event that it occurs.

Fraud control activities are generally classified as either preventive (designed to avoid a fraudulent event or transaction at the time of initial occurrence) or detective (designed to discover a fraudulent event or transaction after the initial processing has occurred). The selection, development, implementation, and monitoring of fraud preventive and fraud detective control activities are crucial elements of managing fraud risk. Fraud control activities are documented with descriptions of the identified fraud risk and scheme, the fraud control activity are designed to mitigate the fraud risk, and the identification of those responsible for the fraud control activity.

Fraud control activities are integral to the ongoing fraud risk assessment component of internal control. Management can either select, develop, and/or deploy preventive and detective fraud control activities to mitigate the risk of fraud events occurring or not being control detected in a timely manner. Control activities cannot provide absolute assurance against fraud. As a result, the department's management should ensure that the organization develops and implements a system for prompt, competent, and confidential review, investigation, and resolution of instances of non-compliance and allegations involving fraud and misconduct.

An organization can improve its chances of loss recovery, while minimizing exposure to litigation and damage to reputation, by establishing and carefully pre-planning investigation and corrective action processes. The organization establishes a communication process to obtain information about potential fraud and deploys a coordinated approach to investigation and corrective action to address fraud appropriately and in a timely manner.

The fifth fraud risk management principle relates to monitoring the overall fraud risk management process. Organizations use fraud risk management monitoring activities to ensure that each of the five principles of fraud risk management is present and functioning as designed and that the organization identifies needed changes in a timely manner. Organizations use ongoing and separate (periodic) evaluations, or some combination of the two, to perform the fraud monitoring activities.

5. RISK RATINGS

Legend used:

Fraud Risk rating	Inherent risk magnitude	Response
16 – 25	High	Unacceptable level of risk - High level of control intervention required /Urgent attention needed.
9 – 15	Medium	Unacceptable level of risk, except under unique circumstances or conditions - Moderate level of control intervention required to achieve an acceptable level of residual risk.
0 – 8	Low	Mostly acceptable - Low level of control intervention required/ If any.

Risk Control Status:

	Risk mitigation control implemented
	Risk mitigation control partially implemented
	Risk mitigation control not implemented

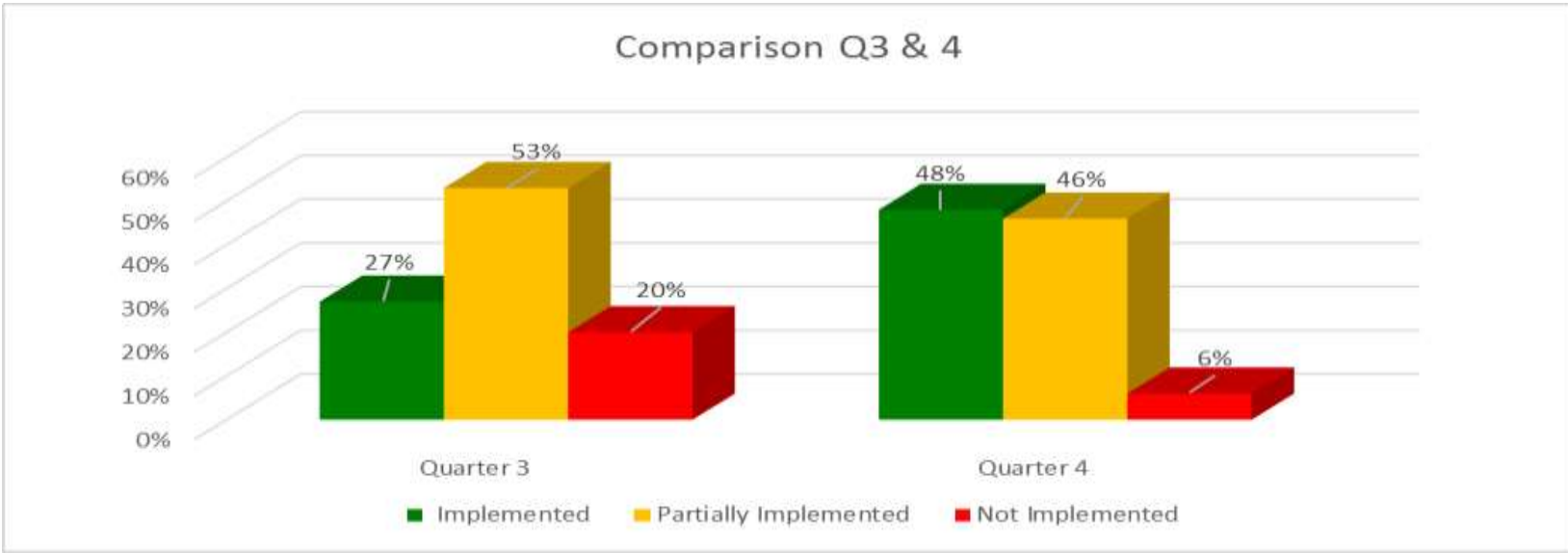
6. LIST OF ASSESSED FRAUD RISKS FOR THE DEPARTMENT

No	RISKS	CONTROL STATUS
1	**Theft of assets:** when an employee steals the goods of the department, either by physically taking it or diverting it in some other way.	
2	**Ghost employee**: when a fake employee or ex-employee is kept on the payroll with pay being diverted to the fraudster	
3	**Leave fraud:** when an employee of the department does not account for actual leave days taken.	
4	Using the department's information to sell for personal gain.	
5	**Theft of Employee Personal information or Contact Lists**: when an employee or departing employee copies or downloads lists of the department's contacts to either sell or use.	
6	**Theft of Personally Identifiable Information (PID)**: when an employee in HR or Finance steals or shares other employees 'credit card numbers or other valuable Personal Identifiable Information (PID) to sell to other parties, example: incurring a stop order on PERSAL without authorization.	
7	**Corruption:** when a contractor, acting on its own or in collusion with the department's employee, substitutes inferior or counterfeit materials for the materials specified in the contract.	

No	RISKS	CONTROL STATUS
8	**Payment Schemes**: when an employee generates a false payment using the Department Service Provider(SP) payment system; or manipulating the account of an existing SP for personal gain	
9	**Overpayment:** when a Service Provider (SP) issues invoices to charge the department for more goods than it delivered or to charge a higher price than agreed; This can be done in collusion with the department's employee, who receives a bribe or by the SP alone to defraud the department.	
10	**Fictitious Supplier:** where an employee in procurement sets up a fake SP account which are paid fraudulent invoices, or initiating the purchase of goods for personal use.	
11	**Theft of Cash**: stealing of assets or petty cash, Example: Personal Use of department assets, when an employee uses department vehicle for unauthorized personal activities.	

7. PROGRESS AND SUMMARY OF FRAUD PREVENTION, RISK MITIGATION FOR 4TH QUARTER

The bar graph below shows fraud prevention, risk mitigation progress of 4th quarter, showing how many were implemented, partially implemented and not implemented:



The above narrative indicates a steady increase in the implementation of the anti-corruption and fraud prevention mitigation actions from Q3 to Q4. Indicating how mitigations actions performed per quarter whether it was implemented, partially implemented or not implemented.

Results of mitigation actions are as follows:

- There are a total of 33 mitigation actions, 16(48%) mitigation actions which were implemented, 14 (42%) which were partially implemented and 2 (6%) mitigations actions which were not implemented for Q4.
- Seven (7) ICT fraud risk mitigation actions were not reported in Q4, due to the open vacancy of the ICT Director.
- It is recommended for the department to fast track the appointment of the ICT Director to minimise the fraud exposure under ICT.

Recommendations of Partially Implemented Mitigation Actions.

There are a total of 15 Partially Implemented Mitigation Actions, 6 of the mitigation actions share the same recommendation as per below:

- The asset verification was conducted and a report was produced, however it is recommended that the report gets communicated and accessible to the business units of Financial Management and Auxiliary and Security Services to ensure shared responsibility.
- Human Resource Management (HRM) has a leave management policy in place, however it was last updated 12 October 2015. It is recommended for HRM to update the policies and procedures as per Public Service Regulation 2016.
- Security scanners are present, however it does not detect metallic or sensitive information. It is recommended for the department to tag confidential and sensitive information to ensure the safety of the department's confidential information.
- The code of conduct exist however the awareness was not created. The code of conduct in the HR policy was last updated in 2016. It is recommended for HR to draft and review a stand-alone code of conduct that includes Youth and Persons with Disabilities.
- The Finance Directorate is implementing segregation of duties in all their processes due to limited staff capacity. It is recommended for Finance to also implement rotation of employees.

- The SCM policy was adopted in December 2019 and it does not express the process of dispute or cancellation of suppliers. It is recommended for SCM to make provision of this clause in their policies/SOP.

Mitigation Actions not implemented and Recommendations

Below are the fraud prevention risk mitigation actions that were not implemented and their recommendations:

Mitigation actions not implemented	**Recommendations**
Investigation processes and procedures for lost and stolen goods are not formally documented.	Auxiliary and Security Services to document and review investigation processes and procedures to ensure consistency and timeous recovery of the lost/stolen goods.
No training and development of SCM staff, however the submission of the training has been approved for the financial year 2021/22	Finance and Supply Chain to ensure that staff are trained and developed in the financial year.

8. STATUS OF FRAUD RISK ASSESSMENT

Fraud Risk	Mitigation Action	Progress on Mitigation	Fraud Mitigation Management Analysis	Control Status
1)Theft of assets: when an employee steals the goods of the department, either by physically taking it or diverting it in some other way.	Asset verification reports should be completed and communicated to Finance/Security.	SCM provided the Q4 Asset verification report.	The asset verification report is completed, however it is recommended that asset verification report gets communicated and accessible to the business units of Finance & Security to ensure shared responsibility.	
	Lost or stolen goods should be registered & investigated	Register for lost/stolen goods is in place.	The register for lost and stolen goods exists and Risk management noted that there were no lost and stolen goods reported for Quarter 4.	

Fraud Risk	Mitigation Action	Progress on Mitigation	Fraud Mitigation Management Analysis	Control Status
	Promote a zero fraud tolerance culture.	Emails are sent through the DWYPD to educate employees on zero fraud tolerance culture and posters are distributed in the department.	Risk management created fraud awareness through emails and posters in Q4.	
	All assets are coded/tagged.	Q4 Asset register classifies all assets with codes or tags.	Q4 Asset register classifies all assets with codes or tags.	
	Disposal of old outdated assets such as laptops, chairs.	Disposal register and committee exists to approve assets for disposals/donations.	Risk management noted that a meeting was held on 21 March 2021, submission for approval of disposal assets were done 30 March 2021.	
2)Ghost employee: when a fake employee or ex-employee is kept on the payroll with pay being diverted to the fraudster	Leave processes should be communicated and followed by all employees.	Leave management report for Q4 was submitted.	Leave management report for Q4 was submitted, however risk management recommends for the policies and procedures of leave management to be communicated to all employees through internet or on other platforms.	
	HR conducts leave audits	HR has conducted the leave audits electronically and leave utilization report was submitted.	Risk management noted that the auditing of leave records were done electronically and submitted to the DG on 17/03/2021.	
3.Leave fraud: when an employee of the	Regular reconciliation of	Leave reconciliation is performed.	-	

Fraud Risk	Mitigation Action	Progress on Mitigation	Fraud Mitigation Management Analysis	Control Status
department does not account for actual leave days taken.	leave forms to biometric report.			
	Maintain and update leave policies and reports	Leave management policy is in place.	Risk management noted that HRM has a leave management policy, however it was last updated in 12 October 2015. It is recommended for HR to update the policies and procedures.	
4.Taking of the department's information to sell for personal gain.	Benchmark with NPI to develop policy on Intellectual Property (IP).	No evidence provided in Q4	No evidence provided.	
	Update the current ICT policy with a clause that expresses "restraint of trade.	ICT Security policy provided.	ICT policy was provided. It is still recommended that ICT policy includes a clause that expresses "restraint of trade	

Fraud Risk	Mitigation Action	Progress on Mitigation	Fraud Mitigation Management Analysis	Control Status
	Establish and formalise a knowledge hub.	No evidence provided	No evidence provided	
	Scanning of employees that make entry and exit from the building.	Security personnel and scanners in place.	Scanning of employees that make entry and exit from the building is done to ensure that security of the department's assets.	
	Tag sensitive information for scanning purposes	Scanners are available for security purposes.	Security scanners are present, however it does not detect metallic or sensitive information. It is recommended for the department to tag confidential and sensitive information to ensure the safety of the department's confidential information.	
	Encrypt classified documents for non-authorised officials	Classified information is encrypted and watermarked.	Classified information is encrypted and watermarked to ensure confidentiality of sensitive information.	
5. Theft of Employee Personal information or Contact Lists: when an employee or departing employee copies or	1) Restrict access to department's sensitive information to only those who	Biometric scanners in place for restricted areas. However they were deactivated to prevent the spread of Covid-19.	The biometric scanners are not working due to covid, risk management noted that A&S has implemented a card security system for authorised access	

Fraud Risk	Mitigation Action	Progress on Mitigation	Fraud Mitigation Management Analysis	Control Status
downloads lists of the department's contacts to either sell or use.	need it in the course of their jobs.		within restricted areas. Risk management recommends the Iris scanner system to tighten the mitigation action.	
	Set up IT controls to alert management of large data downloads or transfers or downloads and transfers that occur at odd times.	Evidence not provided	IT(mitigation actions under the IT Directorate, the progress status for Quarter 4 was not provided due to the position Currently being vacant.)	
	Purchase software that alerts management of suspicious activity on a department network, such as an employee trying to access sensitive information.	Evidence not provided	IT(mitigation actions under the IT Directorate, the progress status for Quarter 4 was not provided due to the position Currently being vacant.)	

Fraud Risk	Mitigation Action	Progress on Mitigation	Fraud Mitigation Management Analysis	Control Status
	Dispose of confidential information properly, by shredding documents and completely removing data from electronic devices before redeploying or disposing them	Shredders are in place	Shredders exist, it was noted that not all of them are working as intended. Risk management encourages for all shredding machines to be maintained for disposal of confidential information	
	Use strong passwords for all computers and devices that can access sensitive information.	Evidence not provided	IT	
	Monitor Clean-desk policy that prohibits employees from keeping sensitive information on their desks while they are not present or not used.	Security management policy in place	It was noted that the clean desk clause is communicated through the use of circulars. It is recommended that clean desk clause be incorporated to Security Management Policy during the review process.	

Fraud Risk	Mitigation Action	Progress on Mitigation	Fraud Mitigation Management Analysis	Control Status
	Limit access to internet or downloads of high volumes of files and printing.	No evidence provided	IT	
6.Corruption: when a contractor, acting on its own or in collusion with the department's employee, substitutes inferior or counterfeit materials for the materials specified in the contract.	Create awareness on the code of conduct for new and existing employees	Code of Conduct exists	The code of conduct exist however the awareness was not created and it was last updated in 2016. It is recommended for the code of conduct to be reviewed to include Youth and Persons with Disabilities and communicate it on the department's intranet or circulars.	
	Implement an investigation process and procedure for employees who use the department's goods for their personal benefit.	Investigation processes and procedures for lost and stolen goods not submitted.	Investigation processes and procedures for lost and stolen goods not submitted by A&S. It is recommended for A&S to document and review investigation processes and procedures.	

Fraud Risk	Mitigation Action	Progress on Mitigation	Fraud Mitigation Management Analysis	Control Status
	Conduct due diligence on all third parties that the department does business with; Finance	State Security Agency (SSA) screening and South African Police Services(SAPS) vetting of employees.	Screening and vetting of employees were done on 9 employees of which 4 employees were screened on January 2021, 2 employees were screened in March 2021.	
	Managers to lead by examples & promote ethical culture through inclusion of an ethical agenda on their meeting.	Ethics management policies and procedures.	Ethics management policy and strategy is in place and communicated to all employees in the department.	
	Train all employees on bribery and corruption prevention	Fraud Prevention e-mails and posters were circulated to all employees.	Fraud Prevention e-mails and posters were circulated to all employees for the purpose of education and training.	

Fraud Risk	Mitigation Action	Progress on Mitigation	Fraud Mitigation Management Analysis	Control Status
7.Payment Schemes: when an employee generates a false payment using the Department Service Provider(SP) payment system; or manipulating the account of an existing SP for personal gain	1) Implement proper segregation of duties between preparers and checkers of payments.	Segregation of duties are carried out in Finance	There is segregation between preparers and checkers of payments within Finance and SCM.	
	2) Rotate duties of employees	No rotation of duties in the business unit.	Risk management noted that the Directorate is implementing segregation of duties in all their processes due to limited staff capacity. Risk management recommends for Finance to also implement rotation of employees.	
	3) Develop and adhere to the department's user (delegated official's) control matrix.	Submission forms to indicate financial delegation of authority.	The financial Delegation of authority was revised November 2020 and again April 2021.	

Fraud Risk	Mitigation Action	Progress on Mitigation	Fraud Mitigation Management Analysis	Control Status
Overpayment: when a Service Provider (SP) issues invoices to charge the department for more goods than it delivered or to charge a higher price than agreed; This can be done in collusion with the dept's employee, who receives a bribe or by the SP alone to defraud the department.	Dispute or cancellation processes should be developed.	SCM policy was submitted.	Risk management noted that the SCM policy adopted in December 2019 does not express the process of dispute or cancellation of suppliers. It is recommended for SCM to make provision of this clause in their policies/SOP.	
	3) There should be proper Segregation of duties (SOD) between the checkers and preparer of SP accounts	No rotation of duties in the business unit.	Risk management noted that the Directorate is implementing segregation of duties in all their processes due to limited staff capacity. Risk management recommends for Finance to also implement rotation of employees.	
	4) Implement a clear delegation of authority (DOA)	Submission forms to indicate financial delegation of authority.	The financial delegation of authority was revised in November 2020 and again in April 2021.	
Fictitious Supplier: where an employee in procurement sets up a fake SP account which are paid fraudulent invoices, or initiating the purchase of goods for personal use	1) Employ and/or train knowledgeable staff to identify suppliers that are not compliant with CSD requirements.	No training & development of SCM staff.	No training and development schedule was done. It is recommended for Finance/SCM to develop and/or train supply chain staff to identify suppliers that are not compliant with CSD requirements.	

Fraud Risk	Mitigation Action	Progress on Mitigation	Fraud Mitigation Management Analysis	Control Status
Theft of Cash: stealing of assets or petty cash, Example: Personal Use of department assets, when an employee uses department vehicle for unauthorized personal activities.	1) Rotate duties of petty cash officials	No rotation of duties in the business unit.	Risk management noted that the Directorate is implementing segregation of duties in all their processes due to limited staff capacity. Risk management recommends for Finance to also implement rotation of employees.	
	2) Reports of spot checks should be readily available.	Petty cash report submitted	The reconciliation file was received, it indicates that petty cash has been reconciled on a weekly basis from 14 January 2021 to 31 March 2021. It is recommended for the Finance Directorate to perform random petty cash counts or spot checks and provide a report.	
	3) Minimum or maximum threshold should be set for cash issued out.	Financial Delegation of Authority	The financial delegation of authority was revised in November 2020 and again in April 2021.	
Payment Fraud: where an employee creates a false bank account to generate false payments; Self-authorizing payments; Colluding with other employees to process false claims for	1) Develop and adhere to the user control matrix to monitor movements of the users in the finance sytem e.g BAS etc	Financial Delegation of Authority	The financial delegation of authority was revised in November 2020 and again in April 2021.	

Fraud Risk	Mitigation Action	Progress on Mitigation	Fraud Mitigation Management Analysis	Control Status
personal gains. **Purchases:** An employee uses the department funds to pay for personal purchases and records the payments as legitimate department's expenses in the accounting system.				
Bribery: an employee participates in a bribery scheme when they accept (or ask for) payments from a Service Provider (SP) in exchange for an advantage	1) Rotate duties of employees in Finance.	No rotation of duties in the business unit.	Risk management noted that the Directorate is implementing segregation of duties in all their processes due to limited staff capacity. Risk management recommends for Finance to also implement rotation of employees.	

9. PROGRESS ON ETHICS MANAGEMENT

The ethical framework are principles of good practice. To determine whether the department has its departmental code of ethics. Ethical values such as professionalism, objectivity, fairness should apply to all employees of the department. Below is progress on ethics management in the department:

- The department has an approved Fraud, Whistleblowing & Ethics Management policies that outlines its focus and commitment to the reduction and possible eradication of incidences of fraud and misconduct. It also confirms the department commitment to legal and regulatory compliance.
- The department has conducted a fraud and anti-corruption risk assessment and produced a register. The fraud register was approved by the Accounting Officer (AC) for implementation.
- Employees are continuously encouraged to report corrupt activities anonymously through National Anti- Corruption Hotline (NACH) of the Public Service Commission (PSC) and through the Department fraud email facility. Risk Management office monitors regularly all the reported fraud and corruption cases through the department fraud email facility and Presidential Hotline. There were no cases reported in the fourth quarter of financial year 2021.
- The number of SMS who are registered for 2020/21 financial disclosure are 39 and 39 SMS have disclosed which means all SMS have submitted their disclosures.
- Values of ethics and integrity are promoted in the fraud awareness circulars and posters.
- Policy on Gifts, Donation and Sponsorship is in place and implemented through the register of gifts and donations.
- Remuneration of work outside the public service, one (1) SMS has applied and permission was granted by the Minister.
- Conflicts of interest are declared in HRM processes and certain Management Committee structures. This will be improved in the financial year 2021/22 through the Management Secretariat.

10. RECOMMENDATION

The following are recommendations from the risk management sub-directorate to instil a culture of “Zero Fraud Tolerance” within the department:

- All alleged fraud and/or corruption should be investigated and all transgressors punished both internally and externally to the fullest possible extent possible.
- Establishment of anti-fraud sub-committees. Their responsibility being to ensure that (a) the Fraud risk assessment within their programmes is conducted (measurement); (b) the fraud response plans are developed; (c) targets and timeframes to deal with specific fraud and/or corruption are set and monitored; and (d) creation of an anti-fraud culture is maintained and fraud awareness is an ongoing process within their programs.
- Every manager in various programs in line with the PFMA, s45, should manage fraud and corruption. a) Each manager should keep statistics of fraud incidence in their area of responsibility that will guide future strategy to fight corruption; b) The department should ensure that fraud prevention is made a measurable performance criteria to all senior managers and captured in their performance agreements