WE CARE WE BELONG WE SERVE

ANTI-CORRUPTION CAPACITY REQUIREMENTS

Guidelines for implementing the Minimum Anti-Corruption Capacity Requirements in Departments and Organisational Components in the Public Service

National Public Service Anti-Corruption Hotline Number
0800 701 701

the dpsa
Department:
Public Service and Administration
REPUBLIC OF SOUTH AFRICA

List of Abbreviations

ACCC	Anti-Corruption Co-ordinating Committee
ASD	Assistant Director
CEU	Code Enforcement Unit
CFO	Chief Financial Officer
CIA	Chief Internal Auditor
CMIS	Corruption Management Information System (DPSA)
DCS	Department Correctional Services
DD	Deputy Director
DDG	Deputy Director-General
DG	Director-General Dir Director
Dir	Director
DIU	Directorate Investigations Unit
dpsa	Department of Public Service and Administration
DSO	Directorate for Special Operations (Scorpions)
dti	Department of Trade and Industry
FAU	Forensic Audit Unit
HR	Human Resource Management
IA	Internal Audit
IMU	Integrity Monitoring Unit
ISU	Integrity Strengthening Unit
MACC	Minimum Anti-Corruption Capacity
NDPP	National Directorate of Public Prosecutions
NIA	National Intelligence Agency
NPA	National Prosecuting Authority
PSC	Public Service Commission
RMO	Risk Management Office
SAMDI	South African Management Development Institute
SAPS	South African Police Services
SIU	Special Investigating Unit

Icons used in the booklet

macc	Extract from the ACCC "Minimum Anti-Corruption Capacity" document	i definition	Definitions
legislation	Relevant legislation	!	Important Points
practice	Examples and case studies from other departments	+ further reading	References to other resources
critical link	Cross references to other parts of the booklet	www	Indicates web addresses

Content

Foreword 2

1. Introduction 3
- 1.1. What is corruption? 3
- 1.2. The Government's response to corruption 5
- 1.3. The Public Service Anti-Corruption Strategy 5
- 1.4. Anti-corruption legislation 6
- 1.5. Improving professional ethics 7
- 1.6. The aim of this booklet 7

2. Developing an integrated anti-corruption strategy 9
- 2.1. What is in an anti-corruption strategy? 9
- 2.2. How to determine a strategy 10
- 2.3. Organisational design and reporting lines 12
- 2.4. Shared service arrangements 20
- 2.5. Information Sharing 21

3. Preventing corruption 22
- 3.1. Ethical organisational culture 22
- 3.2. Policies, Procedures and Internal Controls 27
- 3.3. Training and awareness programmes 31
- 3.4. Physical and information security 36
- 3.5. Verifying qualifications, integrity testing and vetting 38
- 3.6. Corruption risk management 39

4. Detecting corruption 50
- 4.1. Whistleblowing and reporting mechanisms and policies 51
- 4.2. The role of internal audit in detecting corruption 56
- 4.3. Managing information on corruption 58
- 4.4. Reporting to the DPSA 60
- 4.5. The role of managers in preventing corruption 62

5. Investigation 63
- 5.1. Relevant legislation 63
- 5.2. Reporting lines 64
- 5.3. Staff selection 64
- 5.4. The investigation process 65
- 5.5. Investigation methodology 66
- 5.6. Cooperating with law enforcement agencies 72

6. Resolution 75
- 6.1. Disciplinary action 76
- 6.2. Improving controls and prevention measures 79
- 6.3. Referring cases to other agencies 80
- 6.4. Feeding information into the organisation's corruption database 83

7. Bringing it all together 84

8. Conclusion 86

9. Additional Resources 87

10. References 88

Foreword

FOREWORD BY PROFESSOR RICHARD LEVIN, DIRECTOR-GENERAL: DEPARTMENT OF PUBLIC SERVICE AND ADMINISTRATION AND CHAIRPERSON OF THE ANTI-CORRUPTION COORDINATING COMMITTEE

Fighting corruption has been and will remain a priority for our Government. Those of us in the forefront of fighting corruption know that the fight against corruption has many elements and that these must work together in a supportive manner. The Public Service Anti-corruption Strategy advocates that the fight against corruption be conducted in an integrated and coherent manner. This Strategy recognises the importance of detection, prevention and combating; it recognises that solid management practices are as important as the laws that allow investigation and prosecution.

The national Cabinet approved the Strategy in 2002. One of the requirements of the Strategy is that departments and organisational components establish the requisite capacity to prevent and combat corruption in their spheres of operation. During the latter part of 2004 and in the beginning of 2005 an audit was conducted to establish the extent to which departments and organisational components have been able to implement the minimum anti-corruption capacity requirements set by Cabinet. This audit also asked departments to identify the support they need in order to successfully and effectively implement the requirements. The majority of departments requested support in the form of practical guidelines and training.

This guide is the response to the need articulated by departments. It is a compilation of practical examples and experience, from the South African Public Service, on how the requirements have been implemented. This guide will also underpin the practice-oriented skills transfer that will take place in the Public Service during 2006 when a range of training opportunities will be rolled out at national and provincial levels.

The guide is a resource that has been developed for use by anti-corruption practitioners and those setting up or improving the anti-corruption capacity in departments. You are welcome to make copies of the guide or download the e-version from www.dpsa.gov.za/macc/. Similarly, you are encouraged to forward your particulars to bletageng@dpsa.gov.za so that you will receive future additional information on fighting corruption.

The preamble of the United Nations Convention against Corruption states that corruption threatens the stability and security of societies, it undermines the institutions and values of democracy, ethical values and justice and it jeopardises sustainable development and the rule of law. It also robs our citizens, the poor and vulnerable and also those more fortunate, of the services and benefits of our Government. Let us fight this scourge.

PROF RM LEVIN January 2006

1. Introduction

1.1. What is corruption?

Corruption takes many forms. Although the legal definition of corruption is found in the **Prevention and Combating of Corrupt Activities Act (12 of 2004)**, most members of the public understand the word corruption much more broadly to include the abuse of resources, maladministration, theft and fraud. To ensure the public's faith in the public service, it is crucial to address the risks of any these occurring as well as addressing the risks of corruption as defined in the Act. Even 'minor' transgressions like small scale theft, misuse or abuse of property, abuse of sick leave, or generally failing to comply with laws, rules and regulations can have a major effect. And tolerating small scale transgressions often creates an environment for larger scale irregularities to take place.

legislation

The **Prevention and Combating of Corrupt Activities Act (12 of 2004)**.

This Act creates a **general offence** of corruption – which can be committed by anyone whether they are in the public service or in the private sector. It goes on to define specific types of corrupt activities.

The definitions for these offences in the Act are all highly legalistic, but they can be summarised as follows:

Corruption is where one person (A) gives someone in a position of power (B) something (called a 'gratification' in the Act) to use that power, illegally and unfairly, to the advantage of B. As a result, at least two people are needed for the crime to take place, and both will be guilty of the same crime – corruption.

Of particular importance for readers of this booklet are those specific criminal offences (crimes) aimed at combating corruption in the public service. They are:

- Section 4 – Offences where public officials are involved.
- Section 5 – offences where a foreign public official is involved.
- Section 6 – Offences where an agent (someone acting on behalf of someone else) is involved.
- Section 12 – Offences relating to contracts.
- Section 13 – Offences relating to procuring and withdrawal of tenders.
- Section 17 – Offences committed in relation to acquiring a private interest in a contract or agreement of a public body.

legislation

… continued

- Section 20 – making it an offence to be an accessory to, or after, the crime.
- Section 21 – which deals with attempted corruption, conspiracy to commit corruption and inducing another person to commit an offence.
- Sections 28 – 33 dealing with the register that is created for people committing corruption during procurement and tenders.

Some other interesting features of the Act are:

- Gratification doesn’t have to be money. Instead, a whole range of ‘types’ of gratification is listed (Section 1 (ix)). These include donations, gifts, loans, discounts, status, honour, employment and so on that are used to ‘pay’ for the service the person wants.
- The Act doesn’t only cover the public administration – it also creates offences for Parliamentarians, prosecutors, police and others – including corruption in the private sector (where neither party is a member of the public service).
- Section 34 of the Act requires ‘any person who holds a position of authority’ to report cases of corruption involving R100 000 or more. Failure to do so is a criminal offence.

Corruption in the public service affects the entire country. For example:

1 It undermines the fight against poverty by putting money that is meant for infrastructure and development into the pockets of corrupt officials.

2 Corruption increases the cost of public services and slows down service delivery to the public – going against the Constitution and the Batho Pele principles on service delivery.

3 Countries with reputations for corruption scare off foreign investors, losing valuable foreign currency that could be used for economic development.

4 Because corruption is a crime, corrupt officials have to be prosecuted and perhaps kept in prison, which is expensive and puts an additional burden on the criminal justice system.

The Public Service Anti-Corruption Strategy requires departments to address the following:

- Fraud
- Conflict of interest
- Extortion
- Abuse of power
- Bribery
- Insider trading / abuse of privileged information
- Embezzlement
- Favouritism and nepotism

Throughout this booklet, the term ‘corruption’ is used to include all of these, as well as relevant cases of misconduct.

1.2. *The Government’s response to corruption*

Recognising these dangers, South Africa’s first democratic government decided very quickly to fight against corruption and began its anti-corruption campaign in 1997. This led two years later to the first National Anti-Corruption Summit (1999) and, in January 2002, to the **Public Service Anti-Corruption Strategy.**

1.3. *The Public Service Anti-Corruption Strategy*

This strategy is aimed at fighting corruption in an holistic and preventative manner. It contains the following proposals:

1. Review and consolidation of the legislative framework relating to corruption.
2. Increased institutional capacity. This includes the need for departments to create a minimum capacity to fight corruption – which is what this booklet addresses.
3. Improved access to report wrongdoing and protection of whistleblowers and witnesses.
4. Prohibition of corrupt individuals and businesses.
5. Improved management policies and practices.
6. Managing professional ethics.
7. Partnerships with stakeholders.
8. Social analysis, research and policy advocacy.
9. Awareness, training and education.

1.4. *Anti-corruption legislation*

Parliament has passed various laws and regulations to support the government's fight against corruption, including:

- **The Prevention and Combating of Corrupt Activities Act (No. 12 of 2004)**
  As mentioned, this Act provides the legal definition of corruption and creates a range of offences. It also allows for people found guilty of certain offences (such as those related to tenders) to be 'blacklisted' and it requires senior officials to report corrupt activities.
- **The Promotion of Access to Information Act (No. 2 of 2000)**
  This Act gives effect to Section 32 of the Constitution (Access to Information) by setting out how anyone can get access to information held by the state. By so doing, it promotes transparency and prevents government from operating in secret.
- **The Promotion of Administrative Justice Act (No. 3 of 2000)**
  This Act gives effect to Section 33 of the Constitution (Just Administrative Action). It ensures that decisions that affect the public are taken in a way that is procedurally fair and it gives people the right to request written reasons for decisions they disagree with. In this way, it creates greater transparency - people may be less tempted to act corruptly if they know they will have to explain themselves to the public.
- **The Protected Disclosures Act (PDA) (No. 26 of 2000)**
  The PDA (often called the 'Whistleblowers Act) was passed to encourage employees to disclose information about unlawful and irregular behaviour in the workplace. It offers protection from victimisation for 'whistleblowers', as long as they meet the requirements and follow the procedure set out in the Act. This act was under revision at the time of the compilation of this booklet (January 2006).
- **The Public Finance Management Act (PFMA) (No. 1 of 1999)**
  and the **Municipal Finance Management Act (MFMA) (No. 56 of 2003)**
  These Acts set out the requirements for dealing with public finances at the national, provincial and local government levels.
- **The Financial Intelligence Centre Act (FICA) (No. 38 of 2001)**
  This Act creates the Financial Intelligence Centre and was designed to combat money laundering.

1.5. *Improving professional ethics*

Various initiatives have also been launched to improve the level of professional ethics in the public service, including:

- **The Public Service Code of Conduct**
  This code of conduct sets the standards of integrity for public servants.
- **The Batho Pele (People First) Principles**
  These 8 principles set out the required levels of professional ethics in the public service in terms of service delivery.

www www.dpsa.gov.za/batho-pele/

1.6. *The aim of this booklet*

Implementing the minimum anti-corruption capacity requirements

As mentioned, the Public Service Anti-corruption Strategy was introduced in 2002 to specifically address corruption in the public service. As part of the implementation of the Strategy, Cabinet decided in September 2003 to require all public service departments and entities to have a certain 'minimum level of anti-corruption capacity'.

This booklet provides guidelines on how to create this 'minimum anti-corruption capacity'. It aims to assist managers and other officials in the public service tasked with implementing the minimum anti-corruption capacity requirements in their departments. It will also be helpful for anyone who has an oversight role over these functions and any other roleplayers in an anti-corruption strategy.

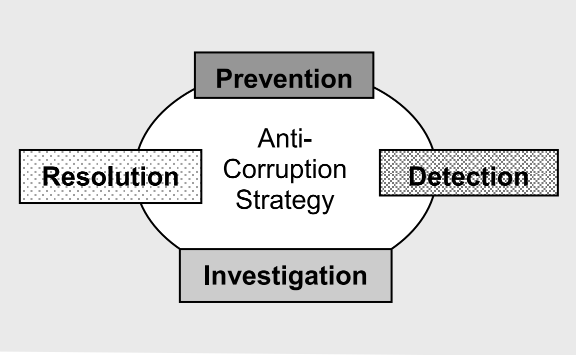
The current structure of your department and the type of strategy you wish to implement will determine who these roleplayers are. It is therefore suggested that all anti-corruption staff read these guidelines to get an understanding of their role within a broader corruption prevention strategy.

Anti-corruption roleplayers
Anti-corruption 'roleplayers' include (but are not limited to) the following functional areas:

- Corporate Governance
- Risk management
- Ethics / organisational integrity
- Compliance
- Anti-corruption
- Internal audit
- Legal
- Human resources

The guidelines in this booklet set out a comprehensive anti-corruption strategy organised around four main components:

- Prevention of corruption.
- Detection of corruption.
- Investigation of corruption.
- Resolution of corruption.



The booklet shows how to integrate these components into an effective anti-corruption strategy for any department. It deals with the need for and objectives of each aspect of the anti-corruption capacity and introduces mechanisms to use with each aspect. It highlights 'good practice examples' from departments that have already implemented the Minimum Anti-Corruption Capacity requirements to varying degrees - and it provides references to other useful information in the fight against corruption.

Although **all** departments must have capacity in **all** of these areas, it is up to each department to decide how they will establish their capacity.

Good practice examples

While this booklet cannot set out a 'one-size-fits-all' strategy, it does include many case studies to show examples of best practice that others can learn from. These are not printed in full - instead, relevant parts of them are highlighted. Where one of these solutions or approaches might suit your department's needs, you should contact the department referred to for more information.

The capacity that Cabinet requires to be in place is set out in an Anti-Corruption Co-ordinating Committee (ACCC) document called: "Minimum anti-corruption capacity for departments and organisational components in the public service". This has been abbreviated to **MACC** and extracts are quoted from it in boxes like this.

2. Developing an integrated anti-corruption strategy

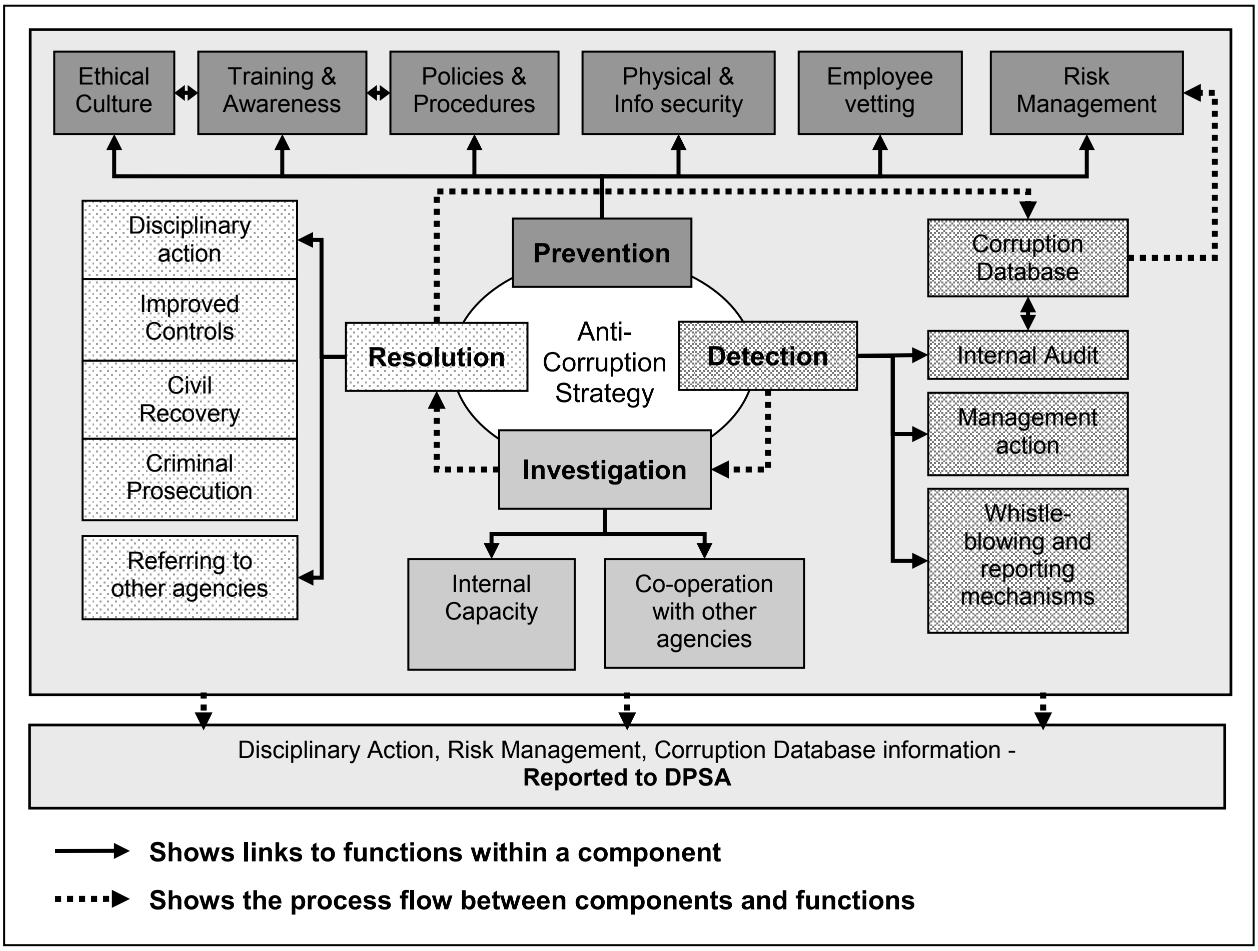
Most departments today are strategy-driven. A strategy provides a route for taking an organisation from where it is to where it wants to go. In the same way, an anti-corruption strategy is the route that an organisation follows to reach its anti-corruption objectives.

2.1. *What is in an anti-corruption strategy?*

An anti-corruption strategy (or fraud and corruption prevention strategy as some departments call it) will address at least the following:

- Your department's objectives regarding corruption. This is usually a commitment to sound corporate governance and a zero tolerance policy towards corruption.
- The corruption risks that need to be addressed.
- The specific anti-corruption components and functions that need to be established.
- Who will be responsible for implementing the various functions. This could include setting up an anti-corruption unit (known by various names such as Anti-Corruption Unit, Integrity Strengthening Unit, Fraud Awareness and Investigations or Departmental Investigations Unit).
- Who is responsible for oversight and monitoring of the process.

The diagram on the next page shows the 4 main **components** (prevention, detection, investigation, and resolution) of an integrated strategy, as well as the various **functions** (or mechanisms) that fall under each component (such as risk management, training and disciplinary action). It also shows the interrelationship between these functions, which is just as important as the functions themselves.

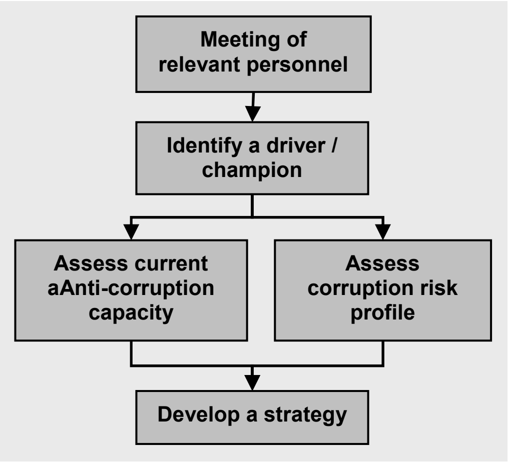


Each of these components and functions is discussed separately in this booklet.

2.2. *How to determine a strategy*

This booklet works on the assumption that your department has taken no steps yet to implement the minimum capacity requirements and sets out a step-by-step process to implement these.

The diagram on the right outlines the process for determining an organisation's anti-corruption strategy:


Meeting of relevant personnel
Identify a driver / champion
Assess current aAnti-corruption capacity
Assess corruption risk profile
Develop a strategy

The following steps are suggested to develop an anti-corruption strategy:

1. An initial meeting is held with all relevant personnel. It is best to have all the relevant parties on-board as early as possible in the process to ensure buy-in from them.
2. A person (or a group of people) must be identified to take responsibility for the process and to drive it forward. While the MACC requirements give the responsibility to ensure that the minimum requirements are met to the Accounting Officer (head of the department or organisation), the implementation is usually delegated. It is however essential that someone (or group) is clearly assigned the responsibility for implementation and that it becomes part of their key performance areas.
3. The organisation’s existing capacity to deal with corruption needs to be assessed. It is possible that many of the anti-corruption functions are already performed in your organisation and that they only need to be integrated into the strategy. During this assessment, you should determine which of the anti-corruption functions can be accommodated in existing functional units, and which of the functions will require new functional units or shared service arrangements.
4. Fraud and corruption risk management is meant to be part of the normal risk management process in all departments. Any fraud and corruption risk assessment you have undertaken should be used to inform your anti-corruption strategy, which must address all of the specific risk areas identified in the risk assessment.

critical link

The process of conducting a fraud and corruption risk assessment is discussed in more detail in the next chapter.

5. An anti-corruption strategy should now be developed based on the minimum anti-corruption capacity functions described in this booklet, your assessment of the current anti-corruption capacity, and the risk assessment.

Once an anti-corruption strategy has been developed, a timeframe must be set for implementing it. This will depend on the size and nature of your department, the resources available, and the current state of ethics and corruption. It should also be remembered that corruption prevention is an ongoing process that needs continuous updating and realignment.

resolution
investigation
detection
prevention

Allocating sufficient resources (people, time, money, and physical resources) is crucial to the success of any strategy. As a result, your anti-corruption strategy should be discussed at your department's strategic planning sessions to prioritise it as an important area in need of resource allocation.

2.3. *Organisational design and reporting lines*

Responsibilities for the various functions to be fulfilled in an anti-corruption strategy must be allocated to specific organisational units. It must be decided how these units will interact with one another, and who they report to on the anti-corruption strategy. The MACC document gives useful guidance in this regard.

macc

Guidelines on structures to accommodate minimum anti-corruption capacity

Departments differ vastly in terms of organisational culture, levels of decentralisation of decision making, location (centrally located, geographical distribution of offices, etc.), size and risk profiles. Departments also have existing organisational capacity that performs some of the required minimum functions. Such capacity may be located in existing anti-corruption units, Internal Audit units, Inspectorate units, and/or Labour Relations units. Executive authorities are responsible to structure departments, and considering this autonomy, existing capacity and the mentioned differences, it is not advisable to prescribe the nature and location of the organisational structures that must ensure the minimum anti-corruption capacity. In view of this, the guidelines below should be considered when departments establish (a) structure(s) to accommodate the minimum anti-corruption capacity:

(a) Departments should consider whether to accommodate the minimum functions in a single anti-corruption unit or to disperse the minimum functions in more than one unit, whether existing or new units. Departments that have regional offices should also consider whether to establish the minimum functions centrally or also in its regional offices. The decision on the nature of the unit(s) should primarily be informed by the corruption risk profile of the department.

(b) Whether departments locate the minimum functions in a single unit or not, responsibilities, accountability and reporting requirements should be clearly defined.

(c) Departments should ensure that the unit(s) responsible for the minimum functions enjoy unfettered access to accounting officers.

(d) Departments that have existing units should assess whether such units can perform the minimum functions.

(e) Whilst it must be recognised that Internal Audit units perform a valuable role in ensuring integrity of internal processes, such units should ideally not perform the minimum functions as such units also have an audit role with regard to the anti-corruption functions and structure(s).

(f) Departments, especially provincial departments, may consider shared capacity.

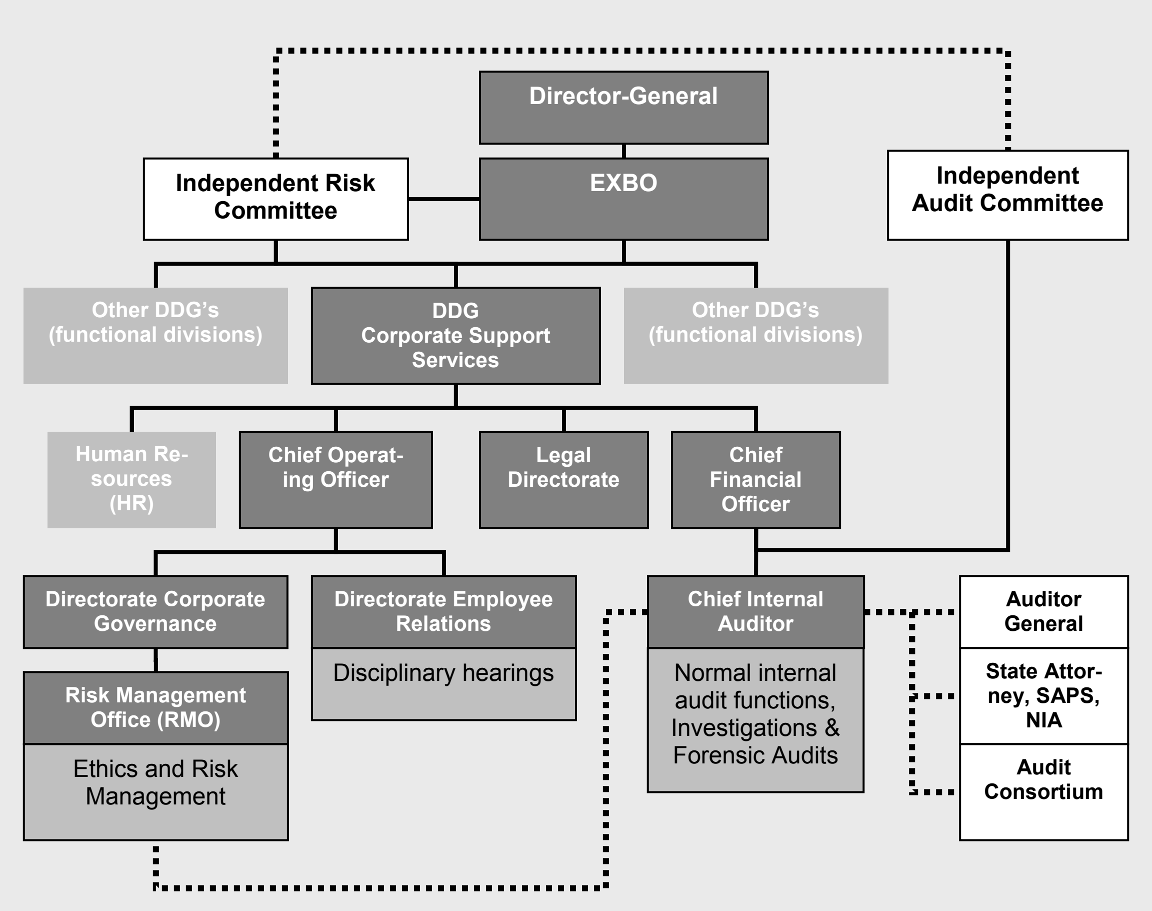
The following examples show how some departments have gone about developing their anti-corruption capacity.

practice

Example 1 - The Department for Trade and Industry (dti)

The Department of Trade and Industry (**dti**)'s anti-corruption management structure is an example of a well-developed capacity that has taken shape over a number of years. The **dti**'s anti-corruption strategy forms an integral part of their strong focus on good corporate governance.

- The **dti** has approximately 800 staff members at Head Office.
- The department is decentralised into four regions.
- There are six divisions in the department itself, each functioning under a divisional head at DDG-level. These six divisional heads form the department's **Executive Board (EXBO)** which is chaired by the DG.



Director-General
Independent Risk Committee
EXBO
Independent Audit Committee
Other DDG's (functional divisions)
DDG Corporate Support Services
Other DDG's (functional divisions)
Human Resources (HR)
Chief Operating Officer
Legal Directorate
Chief Financial Officer
Directorate Corporate Governance
Directorate Employee Relations
Disciplinary hearings
Chief Internal Auditor
Normal internal audit functions, Investigations & Forensic Audits
Auditor General
State Attorney, SAPS, NIA
Audit Consortium
Risk Management Office (RMO)
Ethics and Risk Management

- One of the six divisions is responsible for all **Corporate Support Services** – and most of the anti-corruption capacity falls in this division.

- The **Chief Operating Officer** is responsible for two directorates that have a strong anti-corruption focus **-** Corporate Governance and Employee Relations:
  - **Directorate Corporate Governance** is responsible for the **Risk Management Office**.
  - **Directorate Employment Relations** handles all internal fraud cases and resultant disciplinary hearings.

- The **Risk Management Office (RMO)** (with 2 staff members) is responsible for the following anti-corruption functions:
  - Fraud Prevention Plan
  - Whistleblowing policies
  - Risk assessments
  - Ethics training and awareness
  - Financial Disclosures
  - Receiving information from the National Anti-Corruption Hotline and referring it to relevant authorities.
- The RMO has a dual role - to promote a culture of ethics, and to manage fraud and corruption risks in a pro-active and structured manner.
- The RMO conducts annual risk assessments in close cooperation with the different functional divisions.
- Although both function independently, a close working relationship exists between the RMO and the office of the Chief Internal Auditor (CIA).

- The **dti** also has a **Risk Management Committee,** which is an independent sub-committee of the department's Executive Board (EXBO). All DDG'S are members of the Risk Management Committee, which is chaired by an independent, non-executive chairperson appointed from outside the department. The Risk Management Committee considers the risk assessment reports and formulates recommendations for final acceptance by the EXBO.

- An independent **Audit Committee** is established in terms of the PFMA. This committee consists of three independent, non-executive members plus the DG.
  The Audit Committee has direct access to the Minister, if circumstances require.
  The DG can **not** serve as the Chairperson of the committee.

- The **Chief Internal Auditor (CIA)** compiles all of the reports to the Audit Committee. The CIA is also responsible for managing forensic investigations into corruption. A **Forensic Audit Consortium** exists to conduct forensic audits, at the request of the CIA, when internal capacity is not available. This includes whistleblowing cases and hotline tip-offs. (Although this role of Internal Audit is not recommended by the MACC requirements, it works well within the **dti** structure.)

- The office of the CIA is supported by a professional **Audit Consortium**. This consortium is appointed by tender to conduct audits when internal capacity is not available.
- The CIA reports audit matters directly to the DG and/or the Audit Committee and not via any other senior manager. (For administrative and management matters, like budgets and staff requests, the CIA reports to the DG via the CFO).
- The CIA also undertakes random audits at the request of senior management or following a tip-off, either internally or with the assistance of the Forensic Audit Consortium.
- As soon as any fraud or corruption is discovered, the CIA immediately refers the matter to the DG. Forensic reports are compiled and the **Legal Unit** becomes involved. If staff members are involved, the Directorate Employment Relations is immediately brought on-board to institute any legal actions. Where necessary, matters are referred to relevant outside agencies (such as the State Attorney, SAPS, NIA, or Scorpions).

practice

Example 2 - Department Correctional Services

This example illustrates how Correctional Services has used its risk assessment and strategy to inform its organisational design.

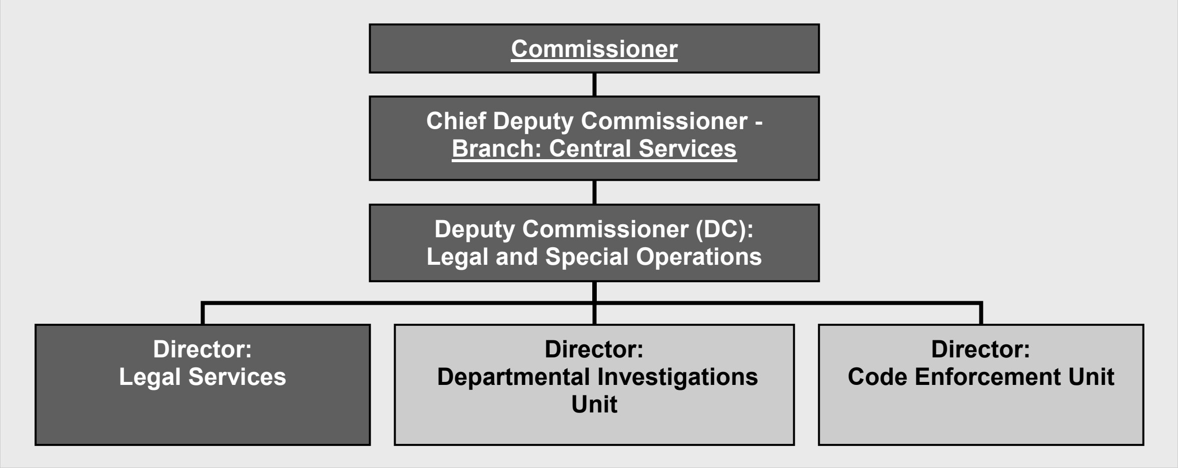
Correctional Services has approximately 35000 staff members. There are 241 correctional centres, grouped into 48 Management Areas. Management Areas are in turn grouped into 6 Regions.

Correctional Services' risk profile shows their greatest corruption risks are at correctional centre and Management Area levels. They have therefore opted for a decentralised *prevention* strategy – emphasising the fact that corruption prevention is the responsibility of the entire department. They prefer not to create the perception that there is a specific unit who will take all the responsibility for corruption prevention and, instead, all managers and staff are required to take ownership of the problem.

The following functions contribute to their strategy:

Risk Management Committee: Correctional Services' Risk Management Committee consists of the 6 Deputy Regional Commissioners, the 16 Deputy Commissioners, the Director Inspectorate and the Director Internal Audit. It is chaired by a Chief Deputy Commissioner (DDG level). Corruption has been identified as one of the 16 risk areas which are monitored at this level. Risk assessment is done annually - in time to inform the department's overall strategic plan. Then, as part of the strategic plan, it becomes the responsibility of management at all correctional facilities and all branches to implement the strategy.

Even though they have adopted a decentralised prevention strategy, the investigation and sanction dimensions are centralised. These are the responsibility of the Departmental Investigations Unit (DIU) and the Code Enforcement Unit (CEU). The following diagram shows how these fit into the department's structure:



Commissioner

Chief Deputy Commissioner - Branch: Central Services

Deputy Commissioner (DC): Legal and Special Operations

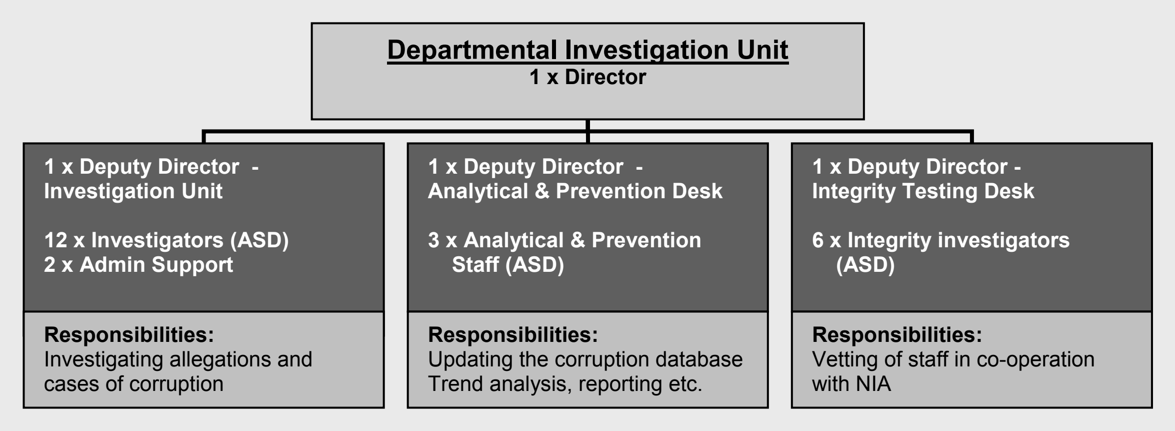
Director: Legal Services

Director: Departmental Investigations Unit

Director: Code Enforcement Unit

Both the DIU and the CEU fall under Legal and Special Operations, who were responsible for driving the development of the corruption prevention framework. They are also tasked with monitoring the effectiveness of all units in implementing Correctional Services' Anti-Corruption framework.

Departmental Investigations Unit (DIU): The DIU has been created specifically to deal with the **detection and investigation** of corruption, fraud and serious maladministration. They have their own hotline but are currently phasing it out in favour of the National Public Service Anti-Corruption Hotline (described on page 52). They also have fax, telephone and e-mail facilities where people can report incidents if fraud, corruption and serious maladministration. Although overseen by the Central Services and Legal and Special Operations, they have relative autonomy within the department regarding investigations. The approach is that all managers should provide the unit with full support in the course of their investigations and non-cooperation with these units is taken seriously.



Departmental Investigation Unit
1 x Director

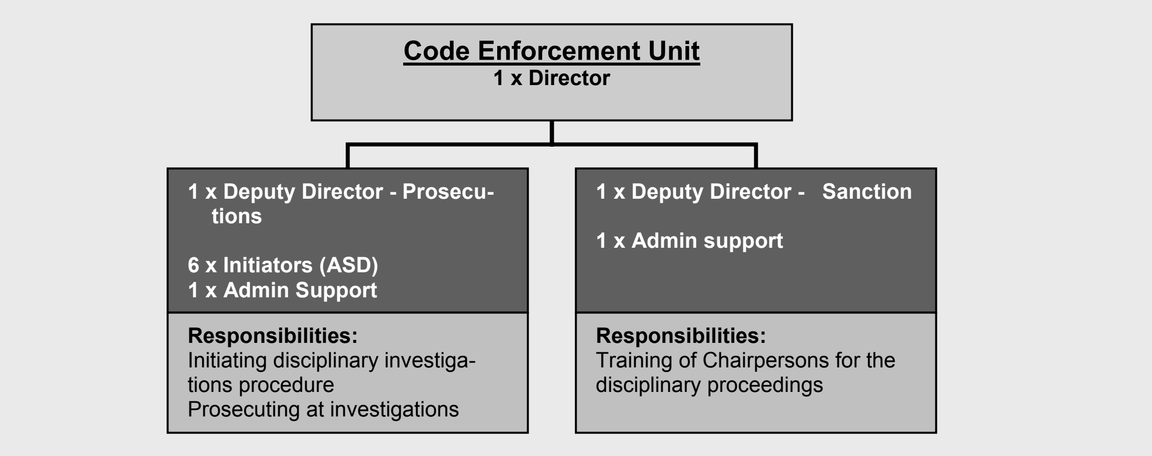
1 x Deputy Director - Investigation Unit
12 x Investigators (ASD)
2 x Admin Support
Responsibilities:
Investigating allegations and cases of corruption

1 x Deputy Director - Analytical & Prevention Desk
3 x Analytical & Prevention Staff (ASD)
Responsibilities:
Updating the corruption database
Trend analysis, reporting etc.

1 x Deputy Director - Integrity Testing Desk
6 x Integrity investigators (ASD)
Responsibilities:
Vetting of staff in co-operation with NIA

The DIU has an **Integrity Testing Desk**, which effectively functions as a Vetting Field Unit in terms of NIA's policy/framework on vetting (assisting NIA to vet staff). It also has an **Analytical and Prevention Desk** responsible for maintaining a database on incidents, doing trend analysis and reporting on this line functionally and to the Executive Management Committee. Information from this database is used to identify high risk areas (to inform the risk management process), as well as correctional centres with high levels of reported incidents, which makes it possible to advise those managers who need to strengthen their anti-corruption focus. This places the responsibility for implementing the strategy back with managers.

Code Enforcement Unit (CEU): Once an investigation has been completed, the file is given to the Prosecutions Unit of the CEU which deals with disciplinary prosecutions. The CEU's Sanction Unit is specifically responsible for training competent chairpersons for disciplinary proceedings.



Code Enforcement Unit
1 x Director

1 x Deputy Director - Prosecutions
6 x Initiators (ASD)
1 x Admin Support
Responsibilities:
Initiating disciplinary investigations procedure
Prosecuting at investigations

1 x Deputy Director - Sanction
1 x Admin support
Responsibilities:
Training of Chairpersons for the disciplinary proceedings

The CEU is also responsible for handing cases over to the SAPS or other external agencies (such as the Scorpions). This happens as soon as there is a suspicion that there might be a criminal case to answer – even if this is during the investigations phase.

The DIU and CEU are situated at the Head Office in Pretoria, but have an anti-corruption function throughout the country. The fact that investigators are not close to the source suits them since it reduces the possibility of intimidation as well as undue influence because of close relationships.

Human Resource Department: HR is responsible for doing pre-employment screening and verifying the qualifications of recruited staff. Anyone found to have false qualifications is dismissed.

Human Resource Development (HRD) is responsible for developing training courses and has included ethics and corruption prevention training as part of the basic training for all new recruits.
HRD also worked with the South African Management Development Institute (SAMDI) and the DIU to develop a course on ethics, code of conduct and corruption prevention for senior managers.

Finance: The Finance Unit is part of the Risk Management Committee and is aware of the strategic importance of this risk area. They are responsible for allocating additional resources when external assistance is required, such as the Special Investigating Unit (SIU), forensic auditors or expert witnesses.

Relationship with the SIU: The SIU assisted in the period when Correctional Services did not have internal investigative capacity as well as with the process of establishing their internal capacity. They continue to play a partnership role in particular in relation to investigations that require technical forensic expertise of a depth that will not be permanently accommodated within Correctional Services. They have already assisted with IT forensic capacity, facilities procurement capacity and pharmaceutical forensic capacity.

The Special Investigating Unit (SIU)

The SIU has been set up to investigate corruption, serious maladministration, improper conduct and unlawful expenditure of public money or property within government departments and other state institutions. It also deals with civil recovery of assets and money and provides advice on disciplinary action. The SIU has through its work with Correctional Services begun to partner with management of government departments in their anti-corruption strategies.

practice

Example 3: Creating a dedicated function

In addition to establishing dedicated anti-corruption structures, specific functions or tasks can be given to existing or new positions. The following is an example of a position that was **specifically** created to perform a corruption prevention function. (Only extracts from the press advertisement are quoted.)

POSITION: DIRECTOR INVESTIGATIONS

REQUIREMENTS: An appropriate B degree or equivalent qualification and extensive experience in managing investigations.

KNOWLEDGE: Relevant experience applicable to the Department; Public Service regulatory frameworks; law enforcement investigations; application of the Minimum Information Security Standards; international instruments on human trafficking and smuggling of immigrants.

KEY PERFORMANCE AREAS:

Development of standards and processes for investigations as well as proposing policy interventions; managing the performance of officials; liaison with various stakeholders; develop an effective case management system; identification and investigation of syndicates; establish and maintain the operational capability of the Directorate; develop, manage, and analyse policies and procedures of enforcement and special investigations; determine training needs in the Directorate.

Note: Short listed candidates will be subjected to competency assessment tests. The appointment will be subject to a positive security clearance and the signing of a performance contract.

“Rendering a world-class service”

Recruitment advertisement for the Department of Home Affairs (Business Times Careers, Sunday Times, November 20, 2005)

2.4. *Shared service arrangements*

Some anti-corruption functions require substantial resources. For example, smaller entities with a low risk profile may find it is not viable for them to establish in-house investigative capacity. Instead, they may prefer a shared service arrangement with another entity, such as the Office of the Premier in their province (if they have capacity), or to use an external agency like the Special Investigating Unit.

Functions that could be shared include:

- Investigations
- Risk management
- Training (although this would need to focus on the specific risk areas of each department)
- Forensic auditing
- Internal audit
- Investigations
- Chairpersons for disciplinary hearings
- The National Public Service Anti-Corruption Hotline - hosted by the Public Service Commission for use by all departments as described on page 52.

Shared service arrangements should be on a long-term basis so that the people delivering the shared service gain an in-depth understanding of all the departments that use their skills.

As can be seen from the following example, many provinces have already set up shared service arrangements with their provincial departments and district municipalities.

practice

An example of shared services: Gauteng Provincial Government

Gauteng Provincial Government has a Shared Service Centre, where a host of services are shared between provincial departments.

Anti-corruption capacity is housed mainly within the Forensic Audit Unit (FAU).

This unit provides the following services to the 12 departments in Gauteng.

- They assist in developing fraud and corruption prevention plans and monitor the updating and implementation of these plans.
- They run anti-corruption training and awareness campaigns throughout the province. This was initially focussed at the management level, but they will soon target other staff members.
- They receive all complaints concerning provincial departments from the National Anti-Corruption Hotline.
- They conduct most of the investigations in the province – although the Gauteng Department of Housing also has investigative capacity and any matters related to housing are referred to them.

Disciplinary action is the responsibility of management in the various departments. The FAU make their investigation reports as well as their investigators available to the affected departments, while the Shared Services' Labour Relations Unit trains presiding officers for hearings.

2.5. *Information Sharing*

Many departments have already taken steps to establish and maintain corruption prevention strategies and are willing to share ideas that other departments can tailor to suit their needs. In this way, knowledge is shared, documents can be made available and capacity can be used across a wider spectrum. For example, trained chairpersons of disciplinary hearings could handle cases for more than one department or in more than one region.

Forums and discussion groups have also been established and regular contact with these can also be valuable. The Anti-Corruption Co-ordinating Committee is one such forum, where all aspects relating to the Public Service Anti-Corruption Strategy are discussed and debated.

Please contact the **dpsa** for references to other departments and relevant forums.

3. Preventing corruption

Prevention is better than cure - particularly when it comes to corruption. Preventing corruption costs far less than investigating it, holding disciplinary inquiries and taking cases to court. It is also good governance practice to focus on maintaining high standards of organisational ethics and managing potential risks in a proactive manner.

It is important to view anti-corruption strategies within a broader context. They are not just about preventing fraud and corruption – they are about establishing and maintaining a culture of ethical and good governance within departments.

The ‘prevention’ component of an anti-corruption strategy is made up of:

- An ethical organisational culture
- Policies, procedures and internal controls
- Training and awareness
- Physical and information security
- Corruption risk management

3.1. *Ethical organisational culture*

An ethical organisational culture is crucial to the success on any anti-corruption strategy, since it is against this backdrop that all the other departmental actions take place. Our ethical values are what we regard as good and bad in our interactions with others. Like people, departments also have (or should have) ethical values. These create its ethical culture and provide guidelines for how every member of the department should behave. For example, if a department’s culture supports service delivery – and this is made visible in everything it does – most staff will start to behave accordingly. If its culture is based on fairness and honesty, employees will expose those that threaten this way of doing things.

Ethical conduct within departments is:

- Required by the Constitution
- The cornerstone of sound governance
- A core responsibility of public office
- An inherent aspect of professionalism
- A major component of organisational success

As individuals, our ethical behaviour is influenced by our personal values. Personal values are formed through various influences including our religious beliefs, culture, gender and economic situation. But when people are employed, their own values might not be enough to deal with some of the grey areas or temptations that they encounter at work. They therefore need to be guided by the values and rules of the department and departments must strive to promote the ethical culture they want to achieve.

An anti-corruption strategy will achieve little success if it is not part of a drive to be an ethical organisation. People should not merely refrain from corrupt behaviour because they fear getting caught - they should refrain from corrupt behaviour because they want to behave ethically. This will only be achieved in departments that actively strive to create an ethical organisational culture.

- ***How can a department's culture be changed?***

Organisational culture can either change naturally and spontaneously, or it can be consciously and deliberately developed. Departments that consciously encourage an ethical culture are usually the more successful ones.

Where to start:

- Encourage people to talk about the department's ethical values and culture and how it should change.
- Engage stakeholders to identify new values that should underpin the department's culture.
- Use any communication methods available to communicate the required ethical values

Management plays a vital role in determining organisational culture – particularly the culture around corruption. If employees do not respect management, the possibility of things going wrong increases. But if management always acts ethically, adheres to policies, procedures and guidelines, and acts strongly and consistently when corruption is discovered, employees will do the same.

REASONS FOR UNETHICAL CONDUCT IN THE PUBLIC SERVICE

Steinberg & Austern identify the following possible reasons for why people act unethically:

- **Good intentions:**

Some public officials do things that they are not supposed to do (or fail to do things that they are meant to do) in an attempt to help others.

- **Ignorance of laws, codes, policies and procedures**

Many public officials simply do not know the laws and directives that deal with what is right and wrong in their work.

- **Ego power trips**

Some employees think they know what is best, regardless of what the department has decided.

- **Greed**

Some individuals exploit their position at work to enrich themselves.

- **It comes with the territory**

Some staff feel there is nothing wrong with using opportunities at work to enrich themselves.

- **Friendship**

In some cases, employees abuse their position in the public service to assist their friends out of a misplaced sense of loyalty.

- **Ideology**

People with strong ideological convictions might believe that any means can be justified as long as it leads to the right outcome for them.

- **Post-employment “revolving door”**

Some public servants engage in unethical behaviour in an attempt to secure a job outside the public service – for example, awarding tenders to certain companies that they hope will employ them in future.

- **Financial problems and pressures**

People with financial problems at home sometimes engage in unethical practises to cope with their problems.

- **Exploiting the exploiters**

Some staff feel that they are being exploited by their bosses and so believe that they are entitled to do anything to turn the tables on their ‘exploiters’.

- **Going along**

Some people feel that, since others act unethically at work, they are entitled to join in.

- **Survival**

Some would do anything to ensure that they maintain and defend their current positions.

- ***Codes of ethics***

Codes of ethics lay down the standards of what is acceptable and unacceptable in the department. They can be either value-based or rule-based (or a combination of these)

Value-based codes of ethics

These are short, aspirational, value-based documents. Many organisations prefer these because they are easy to understand and provide general guidance on how to act ethically. They could refer to values such as honesty, respect, accountability and transparency and state what these values mean to your department.

Rule-based systems, policies, procedures, and processes are then developed to support the code by providing guidelines on specific ethical or anti-corruption issues, like:

- how to deal with gifts (gifts register)
- how to declare interest
- how to deal with sexual or other forms of harassment in the workplace
- how to report fraud, corruption, or other irregularities

Rule-based codes of ethics

Rule-based codes provide specific ethical guidelines or rules for each (or most of) the possible situations that may require ethical guidance. Although they are useful in dealing with specific circumstances, they are often too detailed to provide easy access to information. These codes also foster a 'culture of compliance' where people try to avoid punishment for breaking the rules - unlike a value-based culture where people try to do the right things because they are right.

The Code of Conduct for the Public Service is an example of a rule-based code. Public servants **have** to follow the provisions of the code – if they don't, they may be guilty of misconduct (which is why all staff must be trained on it).

While this code is important, it is a code that is imposed on departments and which might not fully reflect your department's commitment to an ethical culture.

One way of bridging this gap is to include a foreword from the DG or Minister with the Code of Conduct for the Public Service, saying why the code is important to your department. Another option is to supplement it with a value-based Code of Ethics specifically suited to your department's ethical risk areas.

Extract from the Public Service Code of Conduct:

Although the Code of Conduct was drafted to be as comprehensive as possible, it does not provide a detailed standard of conduct. Heads of department are, in terms of section 7(3)(b) of the (Public Service) Act, amongst other things responsible for the efficient management and administration of their departments and the maintenance of discipline. They may therefore, after the matter has been consulted in the appropriate Chamber of the Public Service Bargaining Council, and without derogating from it, ***supplement*** the Code of Conduct provided for in this Chapter in order to provide for their unique circumstances. Heads of department should also ensure that their staff are acquainted with these measures, and that they accept and abide by them.

Codes of Ethics must be living documents - they must be revisited and revised from time to time ensure they reflect the latest developments in your department. It is also important to establish a culture of talking about the code of ethics and its core values whenever decisions are made or actions contemplated. The ultimate goal is to 'internalise' the ethical values in your department to such an extent that they are taken into account without even having to think about it.

+ further reading

Explanatory Manual on the Code of Conduct for the Public Service – PSC

www www.psc.gov.za/codecon.pdf

- ***The role of an 'ethics champion'***

An ethics champion is a well-respected member of top management (or a person that functions close to them) who visibly embodies the department's ethics drive. 'Ownership' of the ethics drive is given to them by top management and they then ensure that the ethics and anti-corruption initiative retains its momentum - and that all the different anti-corruption actions in different parts of the organisation are properly integrated.

Over time and in larger departments, this role may become too big for one person and setting up a more formalised organisational structure might have to be considered.

An ethics champions should be someone with an intimate knowledge of the organisation's business, culture and activities. It should also be someone of high legitimacy and credibility - ideally someone that has facilitated similar initiatives in the past.

3.2. ***Policies, Procedures and Internal Controls***

- ***Aligning practices with values***

An ethical organisational culture does not only depend on value statements. For values to change the way things are done in your department, its policies and procedures must reflect these values. Every policy, strategy, system, process, procedure, and control has to be aligned to creating an ethical culture. This applies to every operational and support function, like HR, finances, procurement, operations, and internal audit.

The support function of HR illustrates this alignment – mainly because of the important role that HR policies, strategies, systems, processes, procedures, and controls play in achieving a department's objectives.

ALIGNMENT OF HR WITH AN ANTI-CORRUPTION STRATEGY

- All HR systems and processes should be **aligned** to promote ethical behaviour in the department or section. This includes recruitment, selection, orientation, training, performance management and disciplinary action.
- The **recruitment** process can be used to inform applicants of how important integrity and ethical behaviour are to the department.
- Only ethical people should be **selected** for employment. This means that honesty and integrity should be considered as vital. Proper background checks are useful and, in some cases psychometric testing for integrity may also be considered.
- New employees **must** be made aware during their initial **orientation** that ethical behaviour is always required and that corruption will **never** be tolerated. New employees may be unaware of the great importance that management attaches to ethical behaviour. If new employees do not know this and come across corruption, they may believe that it is accepted as "the way we do things around here."

ALIGNMENT OF HR WITH AN ANTI-CORRUPTION STRATEGY (continued)

- Employees have to be properly **trained**. They will not automatically know what to do - and not everyone will know what actions are wrong, unacceptable or even corrupt. Unless employees are given, and trained on, clear policies, systems and procedures to guide their actions, things can easily go wrong.

- **Performance management**. Because management must supervise, monitor, guide and direct the performance of employees, they must ensure that staff act ethically at all times. This includes setting appropriate performance guidelines, identifying corrupt behaviour, and immediately taking the necessary actions when things do go wrong.

- **Disciplinary action** when corruption is uncovered is crucial. If immediate, strong and consistent disciplinary action is not taken, it sends a message that corruption is acceptable.

- ***Anti-corruption policies and procedures***

An anti-corruption strategy needs supportive policies to clarify procedures and responsibilities. Examples include:

- **Protected disclosures (whistleblowing) policy.** This policy sets out the procedures and mechanisms for staff to report corruption or malpractice. This is discussed in detail in the next chapter.
- **Gifts policy**. This policy clarifies when it is acceptable to receive gifts and when it is not. It can also deal with how staff must declare gifts in a gifts register.
- A **conflict of interests policy** clarifies what a conflict of interest is, what people should do if they find themselves in a conflict of interest, and how to annually declare their interests. (The financial disclosure of assets and interests is mandatory for all senior managers).
- **Investigations Policy / Terms of Reference for the Investigations Unit**: This sets out the powers and responsibilities of the investigative component, lays down procedures and sets out the protocol to be followed.

- **Disciplinary codes and procedures:** Some departments have included provisions in their standard disciplinary code for serious incidents like fraud and corruption. These provisions must be in line with the Disciplinary Code and Procedures for the Public Service (in Public Service Co-ordinating Bargaining Council, Resolution 2 of 1999).

further reading

Examples of the above policies can be found on the MACC support web-space:

www www.dpsa.gov.za/macc/

practice

NOTES FROM PRACTICE:

The KZN Provincial Treasury has a fraud prevention plan with the following appendices:

- Code of Conduct and Business Ethics
- Disciplinary Code and Procedures
- Fraud Policy and Response Plan
- Whistle Blowing Policy
- Matrix of Tasks and Responsibilities

www www.kzntreasury.gov.za/documents/policies/policies_body.htm

- ***Internal controls***

If there are no security measures in an organisation the chances of theft will be much higher. If someone is allowed to appoint staff at their own discretion, the chances are greater that they might appoint family or friends. And if there is no system for controlling the use of a department’s property, the chances of theft and abuse increase.

The policies, practices and systems that prevent these types of risks are called ‘internal controls’.

definition

Internal controls refer to the policies, practices and systems that an organisation puts in place:

- to provide reasonable assurance that the organisation will achieve its objectives
- to prevent fraud and corruption from occurring;
- to protect their resources from waste, loss, theft or misuse; and
- to ensure that resources are used efficiently and effectively.

Internal controls are usually implemented in specific operational areas of the organisation such as HR, procurement, cash handling and stock control. These controls should be regularly updated and reviewed to ensure that they remain relevant and effective.

National Treasury's **"Risk Management Framework for the Public Service"** identifies the following focus areas for internal controls:

Adequate segregation of duties

- Duties and responsibilities in authorising, processing, recording, and reviewing transactions and events should be separated among individuals and not left to one person.

Custody and accountability for resources

- Access to resources and records must be limited to authorized individuals - who are accountable for their custody or use.

Prompt and proper recording and classification of transactions

- This is done to ensure that information retains its relevance and value to management in controlling operations and decision-making, and to ensure that timely and reliable information is available to management.

Authorization and execution of transactions

- This requires that employees execute their assigned duties in accordance with directives - and within the limitations set by management or legislation.

Documentation

- Internal control policies and procedures, and all transactions and significant events, must be clearly documented.

Management supervision and review

- Competent supervision must be provided - including assignment, review and approval of an employee's work.

They also mention specific computer controls that should be put in place.

critical link

- The strength of internal controls must be assessed during the *Risk Management Process*
- The implementation of internal controls must be evaluated by *Internal Audit*
- Internal controls need to be implemented by people. And so the department's *organisational culture* will have an impact on how consistently internal controls are implemented.
- Once a corruption case has been resolved, the systems must be *analysed* to see whether poor internal controls allowed the incident to take place unnoticed. This must be rectified as soon as possible, and the recommendations shared with other functions in the organisation where similar systems are in place.

further reading

National Treasury's "Risk Management Framework for the Public Service" pp. 47-50

3.3. *Training and awareness programmes*

macc

MACC

"Each accounting officer must establish a training programme (or programmes) that:

- Informs employees on an ongoing basis on what constitutes corruption.
- Promotes the departmental and national policies that must be adhered to, including the values and principles of public administration as contained in the Constitution and standards of professional conduct.
- Informs employees of corruption risks.
- Encourages employees to report corruption.
- Informs employees on the nature and working of protected disclosures and witness protection.
- Informs employees of obligations and rights in terms of the Access to Information and Promotion of Administrative Justice Acts.

Creating ethical awareness among all employees and providing them with proper and continuous training are important in aligning individual behaviour with the department's objectives. Whenever employees are trained on the necessary knowledge, skills, and attitudes to do their jobs well, specific emphasis should be placed on the ethical aspects of their tasks. It should be made clear that ethical behaviour is a key performance criterion and that irregular, fraudulent and corrupt practices will not be tolerated.

- ***Implementing a formal ethics and anti-corruption training programme***

The content

Formal training aims to equip employees with very specific knowledge, skills, and attitudes in the areas mentioned in the MACC requirements (above). This training must cover:

- The need for ethical conduct
- The negative consequences of irregular, fraudulent, or corrupt behaviour for the organisation
- The broad nature of corruption
- Corruption risks. These must be thoroughly addressed and the specific responsibilities of the incumbent in this respect must be clearly spelled out.
- The role of each employee in promoting ethical conduct and preventing fraud and corruption (for example, by reporting corruption). All employees must be trained on the department's whistleblowing policy.
- All of the policies, procedures and controls for a specific task, concentrating on the ethical aspects of it.
- Strategies and processes that the department has put in place to prevent, detect, investigate and resolve ethical breaches or corruption.

Formal ethics and anti-corruption training programme should not just be an add-on to another training programme. While other training programmes might focus on specific line management functions or on broad-based management development, ethics or anti-corruption training should focus on the ethical or anti-corruption aspects of a specific function or task.

Training methods and approach

To equip employees with practical knowledge and skills that are relevant to their actual jobs:

- Ethics training programmes must address real issues that employees face.
- Interactive, participatory training methods should be used and participants should be allowed to share their knowledge, ideas, and experiences.
- Debate and critical thinking should be encouraged and specific decision-making skills should be developed.
- Case studies must be used to illustrate points and participants should be encouraged to discuss specific problems encountered in their own areas of work. Practical solutions should then be developed by the participants.

Who should conduct training?

Since existing training staff might not be equipped to provide such specialised training, the following alternatives can be considered:

Up-skilling existing internal training staff

Existing training staff can be trained to present ethics and anti-corruption training. This training will have to be very thorough, comprehensive and specific and someone specialised may have to assist in designing such a programme. Line managers should also be involved from the start to help customise the programme to specific organisational and functional needs.

Note

SAMDI can assist in training of trainers for departments.

Appointing new staff

Most departments have found it difficult to use existing training staff because of their limited capacity and resources. Because ethics and anti-corruption training is not a once-off event, providing extra capacity for this would be ideal. Some departments have found that financing can be found by prioritising budget needs and submitting well motivated requests to the relevant authorities. In this way, dedicated training capacity can be created.

Using the South African Management Development Institute (SAMDI)

SAMDI is the training arm of the public service. The fact that they provide training to a variety of departments and entities may have the added advantage of developing synergy between different departments - and of developing a mutual understanding of issues relating to ethics and anti-corruption strategies in the public sector.

Using external consultants

Using external consultants is usually discouraged because of the cost and because internal expertise should ideally be developed over a period of time. However, there may be no other option in the short-term.

When using consultants, carefully assess their competence and experience, and check how suitable they are to do training in the public service environment. While previous experience of training for the public service would be a distinct advantage, the goal should always be to ensure at least some transfer of knowledge to staff so that reliance on external consultants can be reduced.

Shared service agreements and networking

As mentioned earlier, some departments have suggested sharing expertise between different departments, either formally or informally. Departments should explore this possibility in their regions before deciding on how much internal capacity they need to build.

- ***Maintaining ethics and anti-corruption awareness at all times***

Awareness of ethics and anti-corruption issues needs to be maintained at all times. Ethics and corruption should form part of the day-to-day talk in the department and management must stress the underlying values and principles at every available opportunity. Information about these issues should be shared with all staff on an ongoing basis and all available means of communication should be used for this.

It is also very important to promote an awareness in the broader community and among all the organisation's stakeholders (for example: clients, suppliers and service providers) that corruption of any kind is not acceptable to the department and that any reports of corruption will be followed up.

practice

Raising awareness

The following methods have been used successfully by departments to raise awareness:

- Direct communication from the minister and DG to all levels of employees at formal meetings and regular informal visits and discussions.
- Properly planned road shows by senior management to the different divisions and sections of the public service.
- Press statements and other media announcements and reports.
- Formal policy documents, procedural guidelines, and other operational documentation.
- Regular in-house newsletters, magazines, or electronic communication networks.
- Existing or specially designed television information screens.
- Specially designed posters, flyers, and other promotional material.

practice

Example: The Department of Public Works

The Department of Public Works has developed a training workshop which is compulsory for all staff at the Assistant Director level and higher (including top management). It deals with the following:

- Raising awareness of the negative impact of corruption, both in the department and nationally.
- The Public Service codes and regulations including the Code of Conduct, disciplinary code, and HR practices.
- Relevant laws (like the Prevention and Combating of Corrupt Activities Act, The Administrative Justice Act and the Public Finance Management Act).
- Risk areas that have been identified within the department.

Training makes extensive use of case studies, which are based on real incidents within the department. Because of their risk areas, they are also planning to conduct more detailed training on the PFMA.

To further raise awareness, the department regularly publishes articles on corruption incidents in their publication (Works News). These mention specific cases as well as the outcomes of these (without mentioning names).

3.4. Physical and information security

Although this could be regarded as an internal control measure, securing your department's physical assets and information deserves separate mention. Not only does it prevent corruption, it symbolises the department's commitment to looking after its own.

Establishing adequate and effective security measures requires specific knowledge, experience, and skills - for example, knowing how to design effective firewalls to protect electronic information. Because it is sometimes necessary to use outside expertise, it is argued that proper safety and security systems are expensive – especially since it involves protecting against something that may never happen. However, even a single security weakness can lead to large scale theft and corruption.

Safeguarding physical assets

Safeguarding an organisation's physical assets means securing at least the following:

- Outside premises and buildings
- Points of entry
- Vaults, safes, storerooms and stock
- Machinery and plant
- Vehicles
- Furniture and artwork
- Fixtures and other office equipment (like air conditioners and computers)

The security risks associated with each of these should be assessed in detail and specific strategies developed to deal with them.

Safeguarding information

Examples of information security lapses include:

- Breaches of confidentiality
- Abuse of privileged information
- Tampering with information
- Misrepresentation of data
- The improper removal of documents (including information in electronic format).

As a result, information that needs to be safeguarded from unauthorised, improper, fraudulent or corrupt use includes:

- Official documents and reports
- Correspondence
- Data bases
- Internal management information systems.

Ways of protecting and safeguarding this information must be put in place, including:

- Firewalls to protect electronic data
- Using passwords for restricted access to privileged information
- Implementing information back-up systems
- A proper document safeguarding process (for example, controlling access to classified information)
- Developing a comprehensive business continuation plan to deal with natural and unnatural disasters (like floods, fires or bomb attacks)

Safeguarding people

Safeguarding people involves taking care of both their physical and psychological safety. In the physical sense, departments must protect employees from physical harm, injury, health threats, raids or violent attacks. In the psychological sense, this means employees must be equipped with the knowledge and skills to safeguard their own work. They should know:

- What to do or say if someone asks them to share confidential information.
- What to do to keep their files and documents safe.
- What to do if they suspect that someone has tampered with their information.

Creating an atmosphere where people feel safe contributes to their willingness to assume ownership and take responsibility for safeguarding the department's assets. Even small measures like a well-managed, user-friendly, and professional entrance control system will help to get this message across.

further reading

The Minimum Information Security Standards set the standard for information security in the public service.

www

www.dpsa.gov.za/macc/

3.5. *Verifying qualifications, integrity testing and vetting*

In theory, the easiest way to prevent corruption is to prevent corrupt employees from entering your department. Although this is simpler said than done, the following will help:

- ***Verifying qualifications***

The qualifications of all staff must be verified. This is usually part of the pre-employment screening process and is the responsibility of the HR unit.

further reading

Additional reading

The Public Service Commission has published a comprehensive guide:

Verification of Qualifications in the Public Service

www **www.psc.gov.za/docs/guidelines/main.html**

Integrity testing

Although controversial, developers of commercial integrity tests claim great success in identifying security risks. But, because honesty and integrity are not easy to assess, these tests are not always accurate. As a result, formal security vetting may be required for some staff.

Security vetting

Security vetting is a process where prospective employees in senior or high-risk positions are formally assessed for security risks by the NIA or Military Intelligence. Because the honesty and integrity of individual employees determine the integrity of the department, security vetting is often crucial. This is especially so for anyone involved in implementing sensitive areas of the anti-corruption strategy (such as investigations).

Although there are limitations to security vetting (the process is slow and the person has usually already started work by the time the results are known), it is still the best way of getting reliable information. Some departments are increasingly submitting job applicants for assessment because of the valuable results they have obtained in the past. Large scale security vetting may also act as a deterrent on its own, stopping corrupt people from applying for high-risk positions in the first place.

Positions that have been identified as high risk areas will need stricter vetting procedures. It is also good practice to link risk profiles to job descriptions to alert the selection committee to the importance of finding a person with high levels of integrity.

3.6. **Corruption risk management**

macc

MACC

Each accounting officer must:

- Specifically focus on and analyse corruption risk as part of the risk assessment required in terms of the PFMA
- Implement fraud plans required in terms of the PFMA, which fraud plans must specifically address the corruption risk

Corruption risk management involves managing the corruption risks that might prevent departments from reaching their objectives. The aim of risk management is to highlight those components of the department that operate in high-risk areas, and to develop a strategy for reducing these risks.

i definition

From National Treasury's "Risk Management Framework for the Public Sector"

Risk is "…the uncertainty of an event occurring that could have an impact on the achievement of objectives. Risk is measured in terms of consequences and likelihood."

Risk management is "…a continuous, proactive and systematic process, effected by a department's executive authority, accounting officer, management and other personnel, applied in strategic planning and across the department, designed to identify potential events that may affect the department, and manage risks to be within its risk tolerance, to provide reasonable assurance regarding the achievement of department objectives."

The MACC requires each department to perform a fraud and corruption risk assessment as part of their normal risk management processes. Departments are also required by the PFMA to develop fraud prevention plans which have to be informed by the risk assessment exercise. A generic fraud and corruption prevention strategy (which is not informed by risk assessment) could lead to an unfocussed attempt at reducing unclear risks.

Different departments have different functions and therefore different risks. For example:

- The Department of Social Development's main risk is in the area of social grants fraud.
- Corruption in housing construction contracts is a risk that impacts on the ability of the Department of Housing to achieve its objectives. Even though these contracts are not managed by the department itself, they need to take steps to mitigate the risk.
- In departments such as Home Affairs, Correctional Services and the South African Police Services, certain staff operate continuously in high corruption risk areas, which will once again require a different approach.

In this Chapter, we look at how departments can assess their own risk areas and develop a comprehensive corruption risk management strategy to meet these specific risks.

- *Who is responsible for risk management?*

Risk management is not the sole responsibility of one individual and various functional areas and staff are expected to play a part.

Accounting officers are responsible for ensuring that risk management takes place in their departments. They are also required to ensure that senior managers incorporate risk management into their management functions.

Senior managers must be aware of the risks in their management areas and must manage these proactively. Much of the responsibility for **implementing** risk management processes lies with them.

Risk management committees are sometimes established to coordinate the department's risk management strategy and manage risk in a structured way. These committees are responsible for risk management across the whole department and report directly to the **Accounting Officer**. Senior managers of each unit (functional or regional) conduct the risk management process and report to the risk management committee. There could also be a **risk officer** to work with senior managers and to assist them with implementing the risk management process in their areas of responsibility.

Internal audit also plays an important role in monitoring:

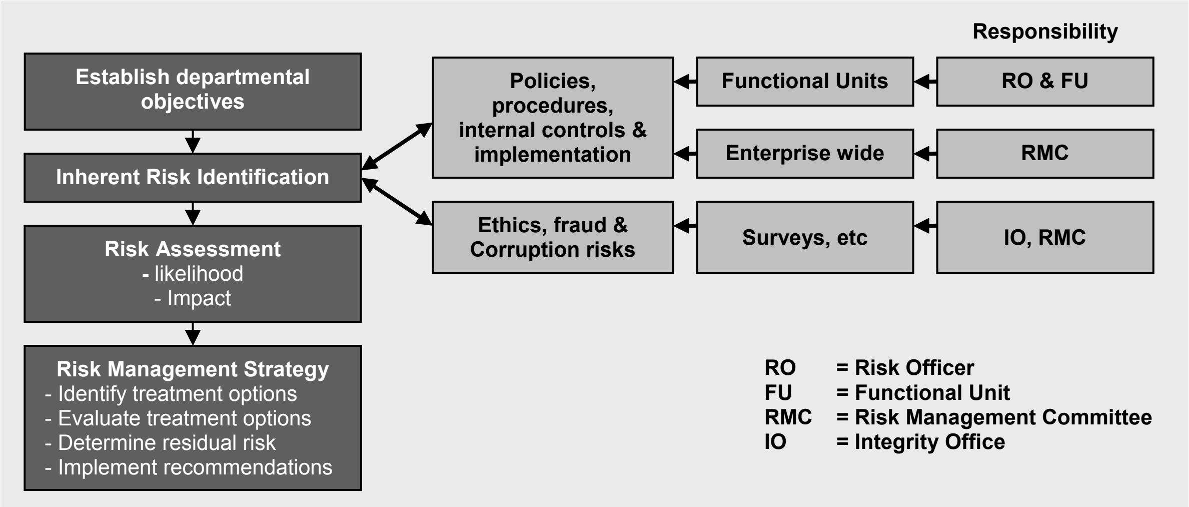
- the effectiveness of the risk management process; and
- the implementation of recommendations to reduce the risks.

Internal Audit usually make their recommendations to the **Audit Committee**. **Internal auditors** can also play a pro-active role in reducing corruption risk by identifying weaknesses in internal controls and suggesting strategies to correct these.

> Everyone involved in risk management must be informed on how to assess corruption risk as part of the normal risk management process.

- ***Overview of the risk management process***

Because there are many different approaches to risk management, only the following key components (which form part of most strategies) will be addressed in this booklet.


Responsibility
Establish departmental objectives
Inherent Risk Identification
Risk Assessment
- likelihood
- Impact
Risk Management Strategy
- Identify treatment options
- Evaluate treatment options
- Determine residual risk
- Implement recommendations
Policies, procedures, internal controls & implementation
Ethics, fraud & Corruption risks
Functional Units
Enterprise wide
Surveys, etc
RO & FU
RMC
IO, RMC
RO = Risk Officer
FU = Functional Unit
RMC = Risk Management Committee
IO = Integrity Office

Getting started

Before conducting a risk assessment, departments should consider:

- What outcome they want to achieve with the assessment.
- What resources are available for it.
- What the time-frames are.

Establish your department's objectives

This should be common knowledge in every department and is usually based on the department's vision and mission statements. Functional units will have their own objectives linked to those of the department. These objectives must be considered to determine which risks could prevent the department from achieving them.

Risk identification and assessment

When identifying risks that might prevent your department from achieving its objectives, don't only focus on material losses the department might suffer. Keep in mind that **any** level of corruption can cause damage to the department's reputation. Corruption risks might not always have a severe impact on delivery in the short term, but if it goes unmanaged it will escalate and become a serious problem in the longer term. And so, there might be risks which have an immediate effect on reaching your objectives, as well as the general risk of a decline in organisational ethics (which should be raised as a separate risk area).

Risks are usually identified on two levels:

- Department-wide risks
- Risks for each operational area

While a risk management committee might be able to assess the department-wide risks from their knowledge of the department, it is best to consult with staff of various operational areas when assessing the risk for their area.

How to assess risk

The Australian standard on fraud and corruption control recommends three methods of assessing risk:

- An independent assessment of processes and procedures - including a series of one-on-one interviews with relevant staff and a review of internal control documentation.
- A fraud and corruption risk survey, using a questionnaire tailored for a specific functional (or business) unit.
- A consultative workshop approach involving as much input as possible from staff of the unit being assessed. 'Risk assessment teams' should be set up for each business unit to identify and assess the risks relevant to their unit.

The workshop approach is preferred for a number of reasons - the most important being:

- Awareness of the risk areas is raised at the operational level right at the start of the process. In the end, the responsibility for managing corruption risks will be at this level.
- Using a consultative process ensures greater ownership and buy-in by staff.

The following areas usually have a high risk:

- Any areas where staff have a lot of discretion and decision-making power.
- Procurement and service contracts (such as a contract to deliver an IT service).
- Inventory management (for example, people who work in the stock room or order stock may need to be carefully managed).
- Sanctions or clearances (for example, people responsible for allocating licences or identity documents)
- Revenue receipt (such as people who receive cash payments from the public).
- Cash management.
- General expenditure.
- Any other areas where staff work directly with the public.

The following table shows examples of risk areas in different functional units within an organisation. It first lists the general organisational risk, and then a corruption or fraud specific risk:

Functional unit	Anti-Corruption Unit	HR	Procurement	IT	Operational
General risk	Lack of succession planning	Long term skills shortage	Lack of skilled contractors	Outdated technology	Lack of resources
Corruption risk	Investigators being bribed / manipulated	Nepotism in appointments	Contract fraud	Fraudulent automated payments	Bribery at the front line

In addition to identifying fraud and corruption risks in your department, it is good practice to also identify and assess any **ethical risk areas**. These are often referred to as 'soft issues', but their impact on your anti-corruption strategy can be severe. Ethical risks are often identified by using a department-wide survey to determine:

- Staff perception of management's ethical commitment
- The level of ethical awareness of staff
- Awareness and application of the Code of Ethics or Code of Conduct
- Awareness of reporting mechanisms
- Staff perceptions of fairness in the organisation
- Whether 'who you know' is more important than 'what you know'
- Whether ethical practices are rewarded in the organisation

practice

Department of Social Development:

Extract from the Anti-Corruption and Fraud Prevention Plan

Fraud Assessment Questionnaire

The ACFP Operational Committee will develop a fraud assessment questionnaire and distribute it to all employees. The purpose of the questionnaire is to:

- Determine the level of awareness
- Determine the level of understanding of anti-corruption and fraud prevention
- Determine the perceptions of employees regarding corruption and fraud
- Determine the level of commitment of employees to curb corruption and fraud

It should, however, be noted that employees have a right to remain anonymous if they wish to do so.

critical link

The information that is gathered by your Corruption Database is vital in identifying risk areas. By doing a trend analysis, you will be able to see what types of complaints are received from which departments. See p. 58 for more on this.

It is good practice to perform the risk assessment process prior to going into the organisations strategic planning. This will enable you to use the risk assessment process to inform the organisational strategy.

Prioritising risk areas

Risk areas identified during your assessment must be prioritised according to:

- The **likelihood** of the risk occurring; and
- The **impact** if it does occur.

The easiest way of doing this is to determine the ‘risk factor’ for each risk. To do this, give a value to the likelihood of it occurring and a value to the impact if it does – then multiply these two numbers. The total will be the risk factor.

Example

Using a scale of 1 – 5 (with 5 being the highest likelihood and the greatest impact), you might find:

- You have a risk that has a high likelihood of occurring (5) but only a relatively low impact if it does (2). The risk factor will be 5 x 2 = 10.
- You have a risk with a medium likelihood of occurring (3) but that will have a major impact if it does (5). The risk factor here will be 3 x 5 = 15 – which means you need to prioritise this risk over that in the first example.

Risk Management Strategy (treating the risks)

Although risks must be dealt with in terms of their priority (with higher risks being treated more urgently and higher up in the organisation), some action must be taken for **each** risk area. This can either be to reduce the chances of the risk occurring, or to reduce the seriousness of the risk if it does occur.

When deciding how to deal with each type of risk, it is important to remember the other elements of your integrated corruption prevention strategy (as shown in the diagram on page 10). You might then choose to focus on any of the following areas:

- Internal controls (which could mean establishing new internal control procedures or updating existing ones). Policies might also need to be updated to increase transparency and oversight over decisions, and to ensure segregation of duties and job rotation in high risk areas. (See p.27)
- Employee vetting and integrity testing. Positions that have been identified as high risk areas will need stricter vetting procedures. It is also good practice to link a risk profile to job descriptions in high risk areas. This will alert the selection committee to the importance of having a person of high integrity in that position. (See p.38)
- Training on internal controls systems and general corruption prevention training can be focussed more aggressively on staff in high risk areas (See p.31).
- Improving physical and information security measures to reduce risks. (See p36)
- Putting procedures in place to detect fraud and corruption at an early stage to minimise the risk. Unscheduled checks, investigations or audits should also be considered for high risk areas. (See chapter 4 on ‘Detection’).

Determining residual risk

Residual risk is the amount of risk left after all of the treatment options have been implemented. While the treatment options chosen might be 100% effective in some areas, other risk areas are not as easy to treat and some residual risk might remain. These areas need to be managed at a strategic level.

Implement recommendations:

This is the most crucial part of the process. If you do not implement the options you have chosen to deal with risks, the entire risk management process will have been a waste of time and resources. Clear responsibilities must be assigned for implementation and those tasked with this must report to the risk management committee on progress.

Monitor and evaluate

Ongoing monitoring and evaluation is essential to make sure treatment measures have been implemented, that they are being followed, and that they are effective. This responsibility can be assigned to the risk management committee although it should also be the responsibility of internal audit.

further reading

Other resources

The Office of the Accountant General at National Treasury has compiled a *Risk Management Framework for the Public Service*. The methodology discussed above corresponds with this framework. It is obtainable from the Office of the Accountant-General's website:

www http://oag.treasury.gov.za/ under 'Publications'

practice

Case Study – The Independent Complaints Directorate (ICD)

A Focus on Prevention

The ICD is a relatively small organisation charged with investigating complaints against SAPS and Metropolitan Police Service members. The ICD National Office is located in Pretoria, but they also have provincial offices. Their risk area is largely at the front-line, where investigators are at risk of being manipulated.

The ICD has taken a proactive approach, not only preventing corruption, but also raising the ethical integrity of the entire organisation. To this end, they have set up an Integrity Strengthening Unit (ISU) consisting of a Deputy Director and an intern. The Deputy Director holds a post-graduate business ethics qualification.

What does the ISU do?

The main purpose of the ISU is to create an ethical organisational culture. They do this in the following ways:

Code of Ethics:

The ISU has developed an aspirational code of ethics to address their specific risk areas. The first step in this process was to speak to staff and external **stakeholders** to find out their ethical concerns and expectations. A full ethical risk assessment was then done and a Code of Ethics was written to clarify the values that are important to the organisation. This consultative process ensured that staff take ownership of the Code and all employees are also trained on the Code of Ethics to make it a 'living document' that people refer to in their daily work.

i definition

Stakeholders are parties that have an interest in a particular department or organisation. They include oversight bodies, employees, suppliers, service providers, clients, interest groups, the media, or anyone else that might be affected by the decisions or actions of the organisation.

Training:

A one-and-a-half day Ethics Workshop was developed, which all staff members (right up to the Executive Officer) are required to attend. This workshop covers:

- The ICD Code of Ethics
- The Protected Disclosure Act
- The ICD's Protected Disclosure's Policy - which explains how to report incidents of misconduct. (The ICD prefer the term 'protected disclosures' because of the possible negative connotations of the term 'whistleblowing').
- The ICD Sexual Harassment Policy

- Typical ethical dilemmas that employees face, such as:
    - Gifts and gratuities
    - Conflicts of interest
    - Confidentiality
    - Permission to do outside work
    - Discrimination (based on the Bill of Rights)

Training makes extensive use of case studies to explain the relevant policies and possible ethical dilemmas. These case studies come mostly from real life incidents to ensure that they are relevant to staff (although they are altered slightly and names are changed so that people don't identify specific situations).

After completing the training, participants must sign a certificate with the learning outcomes of the course to verify that they have received this training and this certificate is then kept on file by the ISU.

The ISU monitors how many new employees enter the organisation and a course is held once there is a sufficient number – with at least one course taking place every two to three months. Ethics training has also been incorporated in the Induction Training Programme, to ensure that staff receive ethics training as soon as possible.

The ISU is also developing a more in-depth 1-day workshop on ethical decision-making skills aimed at managers from Assistant Director level upwards.

Awareness:

The ISU uses various methods to raise ethics awareness, such as:

- An ethics page in the ICD's newsletter
- Small corporate gifts (like rulers and lanyards) with ethics messages
- Ethics messages that appear as 'pop-ups' on computer screens.

These ensure that people are constantly aware of their ethical rights and duties, and help to integrate ethics into the daily practice of the organisation.

Assistance:

The ISU is responsible for receiving all reports of misconduct. They host a 'whistleblowing **helpline**' to advise staff on any ethics matters that they may have doubts about. Typical questions they deal with include:

- Whether or not to accept a certain gift
- How to make a protected disclosure
- Whether or not the caller has experienced sexual harassment.

Because of the sensitive and personal nature of these issues, helpline operators should have some training or experience in counselling or psychology.

Many employees turn to this line for assistance, which shows that staff are starting to take ethics seriously.

The ISU is also developing an ethics library (using the internet and other sources) made up of case studies and guidelines on issues that employees could be faced with (such as conflicts of interest and sexual harassment).

The unit does not just focus on anti-corruption – instead, they believe that by raising ethical awareness, staff will be more inclined to report any incident of misconduct that goes against the values set out in their Code of Ethics.

Alignment of policies:
The head of the ISU gives input on all organisational policies to ensure that they include ethical concerns and are aligned to the organisation's values. This includes going through existing policies to make sure that they are up to date and aligned with each other. They have recently revised their IT policy to clarify the ICD's position on internet and e-mail use and privacy issues.

Dealing with protected disclosures:
The helpline provides assistance and advice and is also used by staff for making protected disclosures. To ensure confidentiality, the telephone line (which is also used as a confidential fax) is separate from the switchboard. Staff and the public also have access to a secure e-mail address to report to. To ensure confidentiality, the ISU has agreed with their IT department that any e-mail that is addressed to, or comes from, this address is not monitored. Since a log is automatically created every time the IT department monitors an address, this log can be checked to ensure that the confidential address has not been monitored. Absolute trust in the integrity of the ISU is crucial to its success and this can only be achieved through ensuring confidentiality in all interactions.

The ISU logs all complaints received onto an electronic database. Some of the complaints are dealt with by the ISU, while others are referred to the relevant functional department for follow-up.

critical link

More information on Corruption Databases appears on page 58 in the 'Detection' chapter of this booklet.

4. Detecting corruption

No matter how successful a corruption prevention campaign is, corruption can still occur. This means that the need to detect corrupt activities, investigate and resolve them will always be part of an integrated anti-corruption strategy. Successfully detecting, investigating and resolving corruption cases also serves as a powerful deterrent to people considering corrupt activities - if people know that they will not get away with corruption they will be less likely to get involved in it.

Be careful of treating all employees like criminals in your attempt to detect corruption. This creates a negative organisational culture, which is contrary to the intention of good governance.

Organisations can only act on corruption that they are aware of. Because corruption is a crime where both parties gain from it, there is very rarely an obvious victim who will be willing to lay a charge. Instead, the victims of corruption (your department – and everyone else in the country) are usually unaware of the crime. This makes corruption very difficult to detect and it is therefore essential to have a proactive corruption detection strategy for your department.

MACC

"Each accounting officer must:

- Establish a system or systems that encourage and allow employees and citizens to report corruption, which system or systems must provide:
    - confidentiality of reporting;
    - the recording of allegations of corruption received through the system or systems; and
    - a formal institutional arrangement for acting on such allegations
- Establish a capacity to detect corruption
- Establish programmes that encourage employees to report corruption
- Establish programmes that inform employees on the nature and working of protected disclosures and witness protection."

Elements of detection

The following are the key elements of a detection strategy:

- Developing a system that encourages employees, clients and the public in general to report corruption. This is discussed under the heading “Whistleblowing and reporting mechanisms.”
- Ensuring that the department’s internal audit function plays a proactive role in the detection of corruption.
- Having a Corruption Database in place.
- Reporting relevant information to the **dpsa** in terms of the MACC

4.1. Whistleblowing and reporting mechanisms and policies

Whistleblowing is the raising of a concern of malpractice in an organisation. People who report corruption are commonly known as ‘whistleblowers’ and a reporting mechanism that makes it easy and safe for people to report is often referred to as a whistleblowers reporting mechanism.

The most effective way of detecting corruption is when people (either staff or people from outside the department) report coming across it in their daily business. Unfortunately though, many people never report misconduct that they see. Studies show various reasons for this, including:

- They did not believe the department would do anything about it.
- Fear of retaliation from management.
- Linked to this fear of retaliation, the lack of an anonymous and confidential means of reporting.

To address this fear, people need to be provided with a safe, confidential and private way of reporting. Some of the ways of doing this are:

- Using the National Public Service Anti-Corruption Hotline
- Internal reporting mechanisms.
- Whistleblowing / protected disclosure policies

resolution
investigation
detection
prevention

The National Public Service Anti-Corruption Hotline

Although some departments have their own internal hotlines, the Public Service Anti-Corruption Strategy aims to consolidate these into a single National Anti-Corruption Hotline. This hotline (which is already in operation) is managed by the Public Service Commission (PSC), which is an independent and impartial institution set up by Chapter 10 of the Constitution (Section 196). Their role is to maintain the highest standard of professional ethics in the public service, which makes them the ideal body to host a hotline of this nature.

National Public Service Anti-Corruption Hotline Number

0800 701 701

This hotline is available 24 hours a day and is independently run and staffed by trained personnel. Calls are logged onto the system and the caller is given a reference number so that they can follow up information without needing to give their name. Reports are then referred to the relevant department to deal with, and departments are required to provide feedback to the PSC on the progress of the matter.

Since this hotline is independently managed, it is one of the safest ways of reporting corruption involving public officials. It is accessible to members of the public (ordinary people, contractors and suppliers dealing with government institutions) to report fraud or corruption **where a government official is involved** – and to public service employees who might prefer to not make use of an internal whistleblowing mechanism.

For information on how to link your department to this hotline, please contact the following people at the PSC:

Mr. J Mudau 012 352 1155 / Mr. R Davids 012 352 1123

Internal reporting mechanisms

Many departments have developed their own reporting mechanisms to allow their staff to report corruption in good faith (where they honestly believe that they saw or uncovered corruption taking place).

When developing such a mechanism, it should be based on the following principles:

- It should be informed by and linked to the Protected Disclosures Act (which has requirements that must be met before the person making the disclosure will be entitled to legal protection).
- According to the MACC requirements, all reporting mechanisms must allow for **confidential reporting**.
- They must offer **real protection** for whistleblowers, especially by ensuring that their confidentiality and identity is protected.
- The **procedures** to be followed must be clear and easy to understand.
- **Confidential guidance and advice** must be made available. The Independent Complaints Directorate case study (p.47) provides a good example of how to provide advice to people who may want to blow the whistle but who are afraid or unsure of the consequences - or who might be unsure whether what they have seen is corruption.
- **Training and awareness** on the reporting mechanism and the Protected Disclosures Act must be provided to all staff.
- An **organisational culture** must be developed of supporting people who report in good faith.

legislation

The **Protected Disclosures Act** (no. 26 of 2000) protects employees in both the private and the public sector who disclose information about unlawful or irregular conduct by their employers or other employees – so called whistleblowers. While it offers protection to whistleblowers, the Act lays out specific procedures that must be followed, and requirements that must be met, before a whistleblower will receive the protection of the Act.

For a disclosure to be protected, the employee who reports the corruption must honestly believe they have observed and the report must be substantially true. When making the disclosure, the employee must follow the routes laid out in the Act, which allows them to report to:

- To a legal advisor
- To their employer
- To a member of Cabinet or Executive Council
- To the Public Protector or Auditor-General
- Other ways, such as to the media, when all else fails.

Each of these routes has their own requirements. Generally though, any disclosure that is made in good faith and according to the employer's procedure (such as a whistleblowing mechanism or policy) qualifies for protection. Even when no policy or procedure is in place, any disclosure made to the employer in good faith is protected.

This act is currently (January 2006) under revision. Be sure to keep up to date with any changes and to keep your department informed.

further reading

The Public Service Commission (PSC) has published an extremely useful booklet on whistleblowing, which is available for download from their website: "*Whistleblowing: A Guide for Public Sector Managers*". The booklet covers:

- Whistleblowing in the South African Context
- Understanding the Protected Disclosures Act
- Putting a whistleblowing policy in place

www **www.psc.gov.za/docs/guidelines/main.html**

Whilst the national anti-corruption hotline plays a vital role, internal mechanisms allow employees to report directly to anti-corruption staff. This has advantages:

- Internal anti-corruption staff members have a better understanding of their own organisational environment. This helps an operator (one of the anti-corruption staff) to ask more appropriate, probing questions. This is crucial, since there is usually only one chance of getting information from the whistleblower.
- The reaction time is usually a lot quicker than when the incident is reported to the national hotline. Speedy reaction is often essential – for example, the report could be about someone already deleting evidence on their computer or about an act of corruption in progress.

Internal mechanisms can include the following confidential facilities:

- Helplines
- fax lines
- e-mail facilities
- Free postal facilities

When creating an internal reporting mechanism, consider the following:

- If you are setting up a helpline, fax machine or e-mail facility, how confidential is it? With e-mails, these should not be monitored by the IT component. Telephone help-lines should be connected to a direct line which is not linked to the department's switchboard.
- How accessible and available is the system? Employees should have a variety of options available to report illegal or irregular conduct, such as a landline, cellular telephone number, fax number and e-mail at any time of the day.

- Are whistleblowing cases dealt with according to clearly communicated standards as set out in your policy? Are all complainants provided with a written acknowledgement of receipt? Timely and continuous feedback is of the utmost importance.
- Are all cases recorded in a confidential database or case management system? Does this system contain sufficient information to assist in identifying trends within your department? This system should also provide accurate statistics for your annual report, as well as for departmental newsletters and other publications.
- Is the ethics officer or helpline interviewer properly trained to deal with confidential and often complex matters in a sensitive manner? For various reasons, many employees prefer not to use answering machines when making disclosures and often merely need to speak to someone who can provide professional advice.
- Are employees trained on the Protected Disclosures Act and do they know how to distinguish between a personal grievance and a protected disclosure made in terms of the Act?
- Are there sufficient procedures or mechanisms in place to ensure the protection of the whistleblower? Top management should publish a written statement that retaliation or victimisation of whistleblowers is considered a serious offence and will not be tolerated.
- Does your department have clear policies on ethical issues (such as gifts and gratuities, conflicts of interest, sexual harassment and insider trading)? Are these policies accessible to all staff? All policies should be available on a central database and employees must be trained on these policies prior to them being implemented.

- ***Whistleblowing policy***

In addition to internal reporting mechanisms, it is also recommended that a whistleblowing policy (informed by the Protected Disclosures Act) be put in place to make sure employees know:

- The various ways of reporting corruption.
- What will happen to their report.
- What protection they can reasonably expect from their organisation.
- The negative effects of malicious reporting, and the actions that will be taken against it.

This policy must be strictly followed at all times especially since, if staff see a whistleblower being victimised, they will be far less likely to report what they see. Your department must be consistent in taking allegations seriously, protecting the identity of people who prefer confidentiality, and following through with investigations, disciplinary actions and other means of resolution.

Being consistent will make people realise that your department has a ‘zero tolerance’ approach to corruption and will encourage them to report. This commitment must be communicated by the actions of all anti-corruption functions, as well as the actions of top management.

www

Web-support:

Samples of whistleblowing / protected disclosures policies can be downloaded from ***www.dpsa.gov.za/macc/***

4.2. ***The role of internal audit in detecting corruption***

The internal audit function’s responsibility is to ensure that the organisation’s financial matters are managed in a responsible way and in compliance with the law. Internal audit:

- Ensures accuracy in the financial processes of the organisation; and
- Checks how credible the organisation’s financial statements are.

It also acts as an internal system of checks and balances and monitors compliance to internal and external guidelines for sound financial management.

Identifying possible areas of risk and formally reporting on these to the relevant authorities is a ‘built-in’ objective of the audit function. The professional nature of the internal auditing task, the formalised working procedures of such a unit, and the requirement that they comply with generally accepted accounting principles usually leads to the detection and reporting of many irregularities.

The internal audit function uses two main methods to perform its task:

Regular planned and scheduled audits

Continuous, regular auditing ensures that internal policies, procedures, and controls are complied with. Through the regular checking of actions, deviations can be uncovered, gaps in procedures identified, and mismanagement or ordinary misconduct uncovered.

Random internal audit checks

Internal audit sections also undertake random audit checks:

- As part of their ordinary working procedures.
- In response to a tip-off or whistleblowing report.
- At the request of senior management.
- To assess a specific risk.
- To assist another function (for example, Risk Management) to devise a specific solution to a specific problem area.

The auditing profession is highly specialised and an internal auditing function can only be run by appropriately qualified staff. The profession is regulated by a range of legal requirements and professional guidelines (primarily the Standards for the Professional Practice of Internal Auditing of the Institute of Internal Auditors). This booklet will therefore not attempt to describe the role of the audit function in any more detail.

4.3. *Managing information on corruption*

MACC

"Each accounting officer must establish an information system that:

- Has a record of all allegations
- Is able to track the progress with the management of each allegation
- Reveals systemic weaknesses and recurring risks, and informs managers and employees of systemic weaknesses/risks
- Provides feedback to employees on the management of corruption allegations
- Provides minimum information to designated national departments."

In order to manage the above information on corruption, a corruption database needs to be established. This is simply a database of all information relating to detected or reported cases of corruption.

The **dpsa** is currently compiling a national database – the Corruption Management Information System (CMIS).

The need for a corruption database

Having a corruption database ensures that:

- All cases are dealt with
- A person has been assigned to deal with the case
- Feedback is received on the progress of the investigation
- Feedback is given to the person who made the allegations
- A record is kept of all incidents
- Trend analysis can be done to inform the corruption risk assessment
- Reports can be given to the accounting officer
- Reports can be given to **dpsa** on an annual basis according to their requirements
- The impact of the corruption prevention strategy can be monitored

Principles of designing and maintaining a corruption database

A corruption database needs to be easy to use and update and at least one person must be assigned the specific responsibility of keeping it up to date. Oversight must be provided to ensure that no cases are lost in the system (which can also be done by using an automatic numbering system). Once an allegation has been logged it may not be removed from the system and, if it is decided not to investigate it, an explanatory note must be provided.

When choosing which fields to capture data on, keep in mind what information you will want from the database at a later stage. To efficiently manage cases and allow for reporting and trend analysis, the following fields are suggested:

- Date of report / detection.
- Person who reported it. This must **not** be filled in if the person has indicated that they would like to remain anonymous.
- Type of corruption. For example, contract fraud, hiring irregularity, tender allocation, accepting a bribe).
- Description of the case / allegations.
- Person assigned to the case.
- Person providing oversight over the case.
- Date assigned.
- Amount involved. This will only apply in cases involving money and may only become available later in the case.
- Ongoing status report. A record should be kept of progress throughout the process, linking progress to specific dates. This could give valuable information showing where the process gets held up.
- Final actions taken. This will give valuable information showing where there are weaknesses in resolving cases.

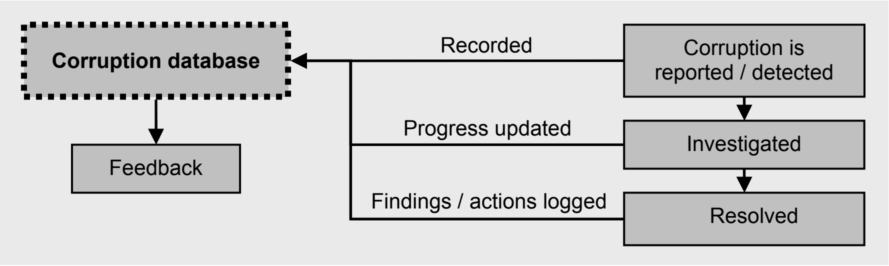
The information on cases and investigations in progress is obviously sensitive, and the information **must** be kept safe and confidential. This applies to **any** information relating to the investigation.

The database does not need to be complicated. Many databases are kept on a simple spreadsheet program, but a database program would be preferable.

While information can be kept in paper form, it is recommended that a computer-based system is developed to make it easier to extract information, compile reports and do trend analyses.

Complainants must be given feedback within a reasonable time so that they know that the matter is being dealt with. This could prevent them from going to the press or other external sources.

General statistical feedback should also be given to staff and other stakeholders to show the successes of the anti-corruption strategy, as well as to alert them to high-risk areas.



*4.4. **Reporting to the*** **dpsa**

One of the minimum anti-corruption capacity requirements is that departments and entities report certain information to the **dpsa** on an annual basis. This information is specified in the following text box. Ensure that information is captured on these aspects in your database on an ongoing basis to make it easy to extract it for reporting purposes.

MACC

“Information on the prevalence of corruption and the efficacy of departmental anti-corruption work is scarce and does not allow for analysis and risk identification on a sectoral or Public Service-wide basis. In order to address these deficiencies, the **dpsa** is establishing baseline information and a central management information system on corruption (Corruption MIS). The baseline and Corruption MIS will assist with compliance monitoring, risk analyses, sharing of information and learning between departments as well as policy improvement and will also aid other bodies such as Parliament and the Public Service Commission with oversight and monitoring and evaluation functions. In addition to this role of the **dpsa**, the National Treasury requires reporting with regard to risk assessment and fraud plans, and the Public Service Commission has the function to monitor and evaluate the application of public administration practices. In this regard the following is required:

(a) Departments provide the **dpsa** with the following information at the end of each financial year:

(i) Number of allegations of corruption, and service delivery areas (e.g. vehicle licensing, award of housing, etc.)

(ii) Number of allegations in (a) handled in terms of disciplinary procedure

(iii) Number of allegations in (a) referred to law enforcement agency or other body

(iv) Number of allegations in (a) not investigated for disciplinary purposes or not referred

(v) The names and relevant particulars (e.g. Persal / identity numbers) of employees and non-employees (e.g. bidder) guilty of corruption.

(vi) Description of corruption risk areas.

(b) Departments certify in its annual report to the National Treasury that corruption risk has been assessed and that the risks are specifically addressed in fraud plans.

4.5. *The role of managers in preventing corruption*

The prevention, detection, investigation, and resolving of fraud and corruption cases is part of the management function of every line manager. None of the suggested strategies limits or lessens this responsibility and line managers must be made fully aware that it is the **non-negotiable** responsibility of line managers to:

- Establish and maintain an ethical culture in their management unit.
- Assess the risk for fraud and corruption in their area of work.
- Put in place policies, strategies, processes and procedures to prevent possible fraud and corruption.
- Put the necessary controls in place to ensure compliance with these policies, strategies, processes and procedures.
- Prevent and detect fraud and corruption.

The final responsibility and accountability for dealing with corruption can never be delegated - but line managers can make use of expert advice and help from others (such as internal auditors, HR specialists, professional risk managers and legal advisers).

5. Investigating corruption

MACC

"Each accounting officer must establish a capacity to investigate allegations"

When possible fraud or corruption have been detected through any of the detection mechanisms discussed in the previous chapter, investigation inevitably has to follow. This requires departments to have a clearly defined investigation procedure. This will be discussed under the following headings:

- The relevant legislation
- Reporting lines
- Staff selection
- The process of investigation
- Methodology
- Cooperation with Law Enforcement Agencies

5.1. *Relevant legislation*

Investigators dealing with corruption will need to be familiar with all of the legislation listed at the beginning of this booklet. This is so they know what legal tools there are to assist in investigations, and what charges can be brought against an accused. In addition the following legislation should also be studied.

- Prevention of Organised Crime Act 1998 (Act 121 of 1998).
- Regulation of Interception of Communications and Provision of Communication-related Information Act 2002 (Act 70 of 2002) – which deals with monitoring employees' communication. Employers need to ensure that they comply with the act before monitoring employees' emails or telephone conversations.
- Witness Protection Act 1998 (Act 112 of 1998) (for witnesses who may require formal witness protection).

5.2. *Reporting lines*

There must be a clear, short communication channel between the Accounting Officer and the Head of Investigations to ensure that there is no chance of interference in the flow of information or investigations. Many investigations have been obstructed by people in the reporting chain who have deliberately blocked, delayed or defeated the course of an investigation. Such people may also try to discredit an investigation unit with the ulterior motive of trying to get it disbanded.

5.3. *Staff selection*

Investigation staff must be specially selected and must have at least a Secret” (preferably “Top Secret”) security classification. These staff may need to be head-hunted for their integrity, perseverance, dedication, honesty, diligence and strength of character.

critical link

See also “Verifying qualifications, integrity testing and vetting” p.38

practice

Notes from practice

Getting a team of competent investigators is always a challenge. When the Department for Correctional Services (DCS) started their investigative capacity, they were under investigation by the Special Investigations Unit (SIU). They entered into an agreement with the SIU that the investigators who were working in the DCS at the time would be available for transfer to the DCS at the end of the process. This allowed them to build up a competent investigative team within the DCS who already had experience of the organisation.

Another approach was taken by the Department: Public Works. They entered into a contract for forensic investigative capacity with a consulting company. One of the conditions of the contract was that the consulting company would transfer skills to the internal investigators within Public Works. During the contract period, the internal and external investigators worked side by side. This had a double benefit.

- Skills were transferred as intended, leaving them with a competent team of investigators.
- The department found that the internal staff complemented the external skills during the contract period because they had a thorough operational knowledge of the organisation.

5.4. *The investigation process*

Who should be involved?

While all corruption cases must be referred to law enforcement agencies, some preliminary investigations will need to be conducted to determine whether there is evidence of corruption having taken place.

Where departments have capacity to do this internally they should do so before reporting it to a law enforcement agency. Where they do not have internal capacity they can call on outside agencies to assist.

- The Special Investigating Unit can be requested to assist in the investigation.
- SAPS can be involved in the investigation so that they ensure that the correct criminal procedures are followed – especially where a lot of money is involved (see text box below).
- In serious cases, the Directorate for Special Operations (Scorpions) might be required.
- In extremely confidential matters, the National Intelligence Agency may have to become involved.

Even where you have internal capacity you could work in co-operation with these agencies. For example, some cases might need special forensic expertise. A partnership with the SIU can provide these resources where it is not viable to create internal capacity in your department.

legislation

Reporting corruption involving more than R100 000

As mentioned, Section 34 of the Prevention and Combating of Corrupt Activities Act requires people in positions of authority (such as the Accounting Officer, or any person in the Senior Management Service) who know (or should have known) that an offence has been committed involving an amount of R 100 000 or more to the police. **Failure to do so is a criminal offence.**

What approach should be followed?

Two options exist when investigating corruption – the suspect could be investigated **overtly** (openly) or **covertly** (in secret). The approach taken will depend on the extent of the corruption and the suspect's status.

Overt investigations can be held where, although serious, the matter is not highly sensitive. Here, the normal reporting channels can be used.

With very sensitive matters though, high-level consultation must take place with the relevant role players to decide on appropriate steps. Usually this would involve a **covert** investigation.

The advantage of using **covert** investigations is that they don't expose the person to coverage in the media that could destroy an innocent person's reputation. It should always be remembered that the purpose of any investigation is not only to prosecute the guilty but also to protect the innocent. Many innocent people have been the victims of malicious, unfounded and offensive allegations – particularly in anonymous complaints where the truth of the allegations can't always be checked. **If it is decided to conduct a covert investigation, then SAPS or the Scorpions must be involved immediately because only they have special authority and powers to conduct covert investigations.**

5.5. *Investigation methodology*

This booklet will only deal with internal investigations of an overt nature, as this is the only type of investigation that departments may conduct on their own.

A. Pre-investigation activities

Before any investigation takes place, the nature of the allegation and the departments and agencies involved must be determined. During this, people in the relevant departments should be involved on a "need to know" basis. An investigation plan should be developed and initial steps taken to secure evidence and information.

practice

Correctional Services' pre-investigation activities

The Department of Correctional Services use the following process during pre-investigation:

1. Debrief the first informant or complainant fully. Establish exactly what the allegation is all about. This is done by interviewing the witness in a structured way and allowing them to relate the story without interruptions while making careful notes.
2. Instruct the first informant of complainant that they should not speak to anyone else about the matter that is being investigated, without first consulting.
3. Establish which department is involved by the nature of the matter being investigated. (For example, the Purchasing Department or Parole Office).
4. Establish the names and functional responsibilities listed in 3.
5. Apply the "Need to Know" principle. Decide who will have to be consulted from the list of names mentioned in point 4.
6. Construct a plan of investigation. (For example, "begin in Accounting Department; interviewing Accountant Mr X; request his assistance in doing XYZ; move to the Purchasing Department – interview M or S, etc.
7. Secure all records, archives, computer tapes and personal records of defendants as the first step, then establish what the required documentary evidence will be, from where and whose control it will be obtained and how it will be safeguarded. The people listed here will all have to submit Affidavits when necessary.
8. Decide upon who will give the Unit the initial affidavit, which will not only report the matter, but will set out in detail the system of operation within the department. It should explain how this system was overridden or compromised. This affidavit need only be submitted after the matter has been properly investigated and the factual situation established.

B. Interviewing witnesses (and the suspect)

i. Preparing for the interview

Investigating officers should know as much about their witnesses as possible – both from a personal perspective and from a professional one. They should know:

- If the witness might be a possible suspect.
- Exactly where the witness fits into the investigation.
- Exactly what information they want to get from the witness. To this end, they should prepare a list of questions in advance. Keep in mind to also be open for additional information that you were not expecting.

ii. The interview

The purpose of interviewing witnesses is to get as much information as possible while only giving out information that is necessary for the purpose of the interview. The interviewee (person being interviewed) should be very briefly informed of the reasons for the interview without disclosing any sensitive facts (such as the name of the person under investigation). The interviewee must also be told not to discuss the interview with anyone else or tell anyone what they were asked. Witnesses (as opposed to those suspected of the offence) should also be told that they have nothing to worry about and that the interview is being held to establish the correct facts about what happened.

ADVICE FROM CORRECTIONAL SERVICES

GUIDELINES FOR CONDUCTING AN INTERVIEW

Make the person feel at ease

The interviewer must create a feeling of security and confidence in the interviewee. The interviewer must be at ease and relaxed. A casual conversation can put a person at ease and in the right mood. The purpose of the interview should also be explained to ensure that the interviewee is not kept in the dark. Sincere interest, friendliness and courtesy towards the interviewee often help to reduce tension.

Get the person talking

Ask the interviewee to talk about the problem, situation, grievance or complaint and do not interrupt them unnecessarily. Show your disapproval, approval, consent or surprise by nodding your head or by making encouraging interjections - for example “oh, I see”, or “Really?” or “I understand” or “what happened then?”. Don’t make prejudiced remarks and try to prevent uncomfortable silences.

Listen attentively and observe

Both the interviewer and the interviewee must understand every word spoken. Ideally, the interviewer should use language best understood by the interviewee. Annoying mannerisms (like raising your eyebrows, fidgeting with your hair or cleaning your nails) can create the impression that you are not interested in the interviewee and their story. Take note of emotional facial expressions and non-verbal communication. Remember that a good interviewer is a good listener. Don’t urge the person towards the answer that you want to hear.

Take notes

Take notes during the interview. Tell the interviewee that you are planning to do so and why. Hold your notepad or paper in such a way that the interviewee can't see what you are writing. Only use keywords and learn to note things without losing concentration and while still listening to the interviewee.

Questioning

Questions must be concisely formulated. Avoid discriminating questions. If the interview lends itself to it, plan beforehand what information you want to obtain during the interview and formulate questions to get this information if it is not readily revealed. Avoid asking closed questions – question where the interviewee can only answer “yes” or “no.” Give the interviewee ample time to answer the questions – and don’t answer your own questions.

When interviewing the complainant and other witnesses, investigators must be sure about which potential offences they are dealing with, their definitions, and what the elements of the offences are – that is, what will have to be proved for the person to be found guilty. This allows investigators to make sure that evidence to prove all of the elements of the allegation is obtained from witnesses.

iii. Questioning the suspect

The purpose of questioning the suspect is to establish the facts. Questions should therefore be aimed at establishing any unknown factors and confirming facts supplied by others.

It is important to remember that everyone is innocent until proven guilty and that they should be treated in this way throughout investigation and disciplinary processes.

practice

ADVICE FROM CORRECTIONAL SERVICES

INTERROGATION STRATEGIES

The same techniques do not work for all interrogations. Approaches and questions differ with the type of suspect being questioned and how certain you are that they are guilty of the offence.

When it is clear that they are guilty, warning the suspect to tell the truth and pointing out some of the evidence against them can help to get them to admit their guilt. An empathetic approach can often be successful in getting suspects to admit their guilt – this includes:

- Telling the suspect that anyone might have done what they did under the same circumstances,
- Downplaying the moral seriousness of the offence,
- Suggesting a less offensive motive than the one you suspect.

When a suspect's guilt is uncertain, the interrogator should begin with an indirect approach, assuming that the interrogator already possesses all the necessary facts. By using physical evidence, photographs, and sketches, and challenging lies, the interrogator may make this method extremely productive. When a suspect begins bargaining, it indicates that they accept the reality of their involvement, but only to a limited extent. They will still probably want to share responsibility with others. This is a good time to use techniques that will make it easier for the suspect to accept full responsibility. When the suspect accepts their involvement they may be willing to confess.

C. Statements and affidavits

Once it is clear that an offence has been committed, statements should be taken from all witnesses. These are written records of what witnesses saw or know took place.

i. The complainant's statement

Complainant's statements should always be sworn to – ideally in the form of an affidavit. Affidavits carry more weight than unsworn statements and provide the basis for applying for warrants of arrest, search and seizure.

i definition

Affidavits are legal documents that need a Commissioner of Oaths to sign that the witness has read the statement and swears that its contents are true.

ii. Statements from witnesses

Affidavits should also be taken from witnesses to support the allegations made by the complainant and to strengthen the case against the accused. Together with the complainant's statement, witnesses' statements must address all of the elements of the offence that the person will be charged with. In a sense, they are the 'building blocks' in a case.

Statements must be taken from people who actually witnessed what happened and those who give statements in their official capacity. For example, an auditor may not have witnessed the offence taking place, but they may have conducted an audit and found certain irregularities.

D. Search and seizure

Searches and the seizure of things to be used as evidence (like computers) must be done **strictly** in line with the Constitution and Sections 20 to 36 of the Criminal Procedure Act.

The Constitution protects the rights of its citizens against arrest, seizure and confiscation of their property. There are exceptions that allow this to happen under certain circumstances, the investigation of crime being one. However, the rights of a suspected person are clearly set out and if these are denied or ignored, it could lead to the case being dismissed. It is therefore very important that investigators are aware of the constitutional requirements and that these are carefully observed.

practice

Advice from Correctional Services:

When conducting a search:

1. Draw up flow chart of internal system and a documentary trail.
2. Establish the period to be investigated (for example, the last six months.
3. Gather all identified and required documentary evidence that reflects the transaction flow of the entire system for the whole of the identified period of investigation.
4. It goes without saying that the defendant should be present at all times during the search. If requested, the legal advisor should also be allowed to be present to protect the interest of the client.
5. If possible, use only one (1) person to gather the documentary evidence. This person must note the date, time and place as well as the person from whose control he uplifted the documentary evidence. This person should issue receipts (for documents) and keep copies of the original receipt. Affidavits will be required from each of the persons who handed him the documentary evidence. The person gathering the documentary evidence will also be required to submit an Affidavit stating that they uplifted all the documents, from whom and when this was done
6. Working copies of all uplifted documentary evidence must be made. The originals should then be locked away in a safe place. No marks whatsoever must be made on any original document. An index of documents uplifted, which not only lists these documents, but also explains the nature of each, should be compiled.
7. Any computer evidence should be copied on separate disks by the person normally responsible for operating that computer. If that person happens to be a possible suspect, then copies must be made by any other computer literate person – IN THE PRESENCE OF THE SUSPECT. The copied disks should be sealed in the suspect's presence and safely stored.
8. Affidavits will be required for each step of the way, regarding gathered documentation.
9. The scribe should make a list of everything that was seized. The list should be in duplicate and should describe each article in such detail as to readily identify it. Once the search is over and the list has been completed, the scribe should sign and date each page. The defendant is requested to also likewise sign it and the duplicate is handed over to the defendant.

E. Linking exhibits

The purpose of search and seizure is to find evidence of the commission of the crime being investigated and to link the accused or defendant to the crime. With handwritten documentary evidence, the identity of the author must also be established. It is even possible that fingerprints can be found on some documents, proving the accused touched them at some stage. The success of any investigation depends on protecting the integrity of its exhibits and this must be ensured at all times. This means keeping evidence safe and preventing theft of, or tampering with it.

F. The charge

In criminal procedures the charge will be drawn up by the prosecutor. In internal disciplinary hearings the charge can only be drawn up once the investigation is complete and needs to be based on the evidence (documents, statements of witnesses, etc.) In addition, investigators must have a thorough knowledge of the disciplinary code to know what the accused or defendant should be charged with.

5.6. *Cooperating with law enforcement agencies*

Investigators must have and maintain good working relationships with the following law enforcement agencies:

- South African Police Service
- Special Investigations Unit
- National Prosecuting Authority
- Directorate for Special Operations and Serious Economic Offences (the Scorpions)
- National Intelligence Agency.

Training on the process of investigation should be closely aligned with that of the SAPS. This will avoid delays in matters having to be re-investigated to comply with requirements in court.

Criminal matters should be reported to the relevant agency without delay and all information and exhibits should be placed at their disposal. Assistance should be given to all external investigators and the department should have a clear policy on this since they may need to have access to sensitive information.

Departmental staff who refuse to cooperate with external investigators must not be tolerated. Any refusal to assist should be interpreted as an attempt to defeat the investigation and should be treated with suspension or dismissal.

practice

Example: Department of Correctional Services

The Process Flow for Case Files in the Department of Correctional Services

This is the process proposed by the Department of Correctional Services Directorate Investigations Unit (DIU)

1. Report by complainant

   Reports about the alleged transgressions or corrupt activities will be reported to our toll free line and some complainants or sources of information will report to our offices in person. Reports will also be received by facsimile, memorandums, confidential letters, local newspapers (media) and e-mails.

2. Opening of case files

   Upon receipt of the complaint, the toll centre operator will open a case file, capture it on the IT system, and record it in the control register as a back-up system, whereafter it will be given a unique identification number. The file will then be subjected to a screening process.

3. Inspection of case file by screening officer

   The delegated official will asses the facts with the view to distinguishing as to whether the case warrants DIU involvement or that it should be referred to the regions. If the case does not warrant our involvement the complainant must be informed in writing and the file may be closed and forwarded for archiving.

   - Purpose of screening office:
     - A screening office within the toll free centre must have an experienced investigator, who will screen the cases before they can be allocated to the investigators if it merits DIU investigation.
     - This means that there will constantly be an investigator “on call” to screen case files and attend to more serious matters (preliminary investigations).
   - Procedure to be followed at the screening office:
     - An entry must be made in the investigation diary about all actions carried out during the screening process.
     - Indicate as to whether the case merits DIU intervention and why.
     - If the case does not merit DIU intervention, also state the reason why.
     - Forward the case files to the DD for distribution or closing.

4. Allocation of files to DIU and transfer thereof to various regions

   - The DD of the DIU must assign the case file to the investigator in the DIU control register.
   - The investigator acknowledges receipt of the case file in the DIU register.
   - The investigator will then enter the case in his/her case registers for their further handling.
   - The investigator must compile a preliminary report for the DIU Director’s attention and continue with investigation.
   - The case file must be handed to the DD of the DIU for 24 hours inspection and further dispatch it for brought forward inspection.
   - The investigator must inform the employee who is the subject of an investigation of the investigation against him, the results of which may be used at the disciplinary inquiry.
   - An investigation should be finalised within two weeks from the date that an incident has come to the attention of the employer. If the time frame cannot be met, the parties involved must be informed accordingly with reasons for the delay.

5. Please Note

- Quarterly and annual inspections would be conducted at any stage of the above process.
- The DIU control register and the system must be updated after each of the above inspections has been performed.
- After the case has been finalised and closed it must be handed over to the administration officer who will acknowledge the receipt thereof and archive it accordingly.
- The administration officer should keep the register for all cases archived.

Re-opening of a case file

In cases where there is a complaint that warrants the re-opening of the archived file the following procedure should be followed:
- The administration officer re-opens the case in a DIU control register with a red pen, and the procedure in paragraph 4 should be followed.

6. Investigations

Investigators will pursue the files and decide on the approach in executing the task taking into account the budgetary constraints, speedy resolution, effectiveness and the procedural requirements as envisaged in the department's Disciplinary Code and Procedure.

7. Investigation diary

- Details must be given of person(s) from whom the statements have been taken (names of other witnesses).
- Statements must be filed regarding exhibits that have been confiscated.
- All statements must be clearly marked, for example 'annexure'.
- All given instruction must be acknowledged on the investigation diary.
- All the activities concerning investigation must be noted on the investigation diary from time to time.

8. Conclusion

The process of ensuring effective case control will have the following advantages for the DIU:

- It will improve the distribution of the workload of the investigator;
- It will enhance the accountability of all cases reported; and
- It will give rise to an improved image which will result in higher productivity and effectiveness of investigators.

All this taken into consideration will enable resources to be utilized optimally. Also successful prosecutions will lead to motivated members and give way to a standardised procedure.

6. Resolution

While many organisations focus their anti-corruption capacity on detecting and investigating corruption, resolution is often left to chance. Yet, if corruption cases are not successfully resolved, all the effort you have put in up to this point will have gone to waste. Besides being demoralising for the rest of the anti-corruption components, it also sets a bad precedent if the resolution component fails. People with corrupt intent will not be deterred if they know that they will get off lightly.

As a result, special attention should be given to making sure your department has the capacity to resolve matters successfully. This means allocating responsibilities and resources to this component, and developing or acquiring the relevant skills.

Note

Some of the skills for resolving cases can be acquired through shared service arrangements and through reporting cases to law enforcement agencies.

Although you should have a policy to say who decides on which resolution mechanism to use and where to refer cases, the usual process is for the file and a report with recommendations to be given to the person who has jurisdiction over the investigations unit. Depending on the size of your organisation and the seriousness of the allegations, the file may also be given to the Accounting Officer.

In addition to criminal prosecutions, the following should be considered:

- Disciplinary action
- Improving internal controls
- Recovery of losses

! When reading this Chapter, it must be remembered that **all** cases of corruption **must** be referred to the SAPS or the Scorpions for criminal prosecution. While disciplinary actions are important and incidents of corruption allow you to improve internal controls, these should not be seen as an end to a case of corruption.

6.1. *Disciplinary action*

MACC

"Each accounting officer must establish a capacity to institute and complete disciplinary action for cases of corruption."

Disciplinary action generally refers to the procedures for dealing with staff who have committed work-related misconduct. While **all** cases of corruption must be referred to the SAPS or the Scorpions for criminal prosecution, disciplinary action can be taken against offenders as well. These two processes (criminal prosecution and disciplinary action) can run at the same time - the one does not prevent the other from taking place, and a finding in the one does not have an impact on the finding in the other.

Disciplinary action is usually the responsibility of line management together with the HR or Legal Units. All departments have standard **disciplinary codes**, which are an important part of any corruption prevention and ethics plan. The unit responsible for disciplinary action should also be included in anti-corruption strategy discussions. This will allow them to better understand their responsibility within the broader anti-corruption strategy.

Disciplinary codes:
Departmental disciplinary codes **must** comply with the **Disciplinary Code and Procedures for the Public Service** (in the Public Service Co-ordinating Bargaining Council, Resolution 2 of 1999).

It should also be remembered that, because of the serious effects of corruption, a 'zero-tolerance' approach is required. As a result, it is not advisable to deal with corruption cases in the same manner as minor disciplinary actions. Employees must be made fully aware of the consequences of any transgressions – including both disciplinary action and criminal prosecution. And the procedures used when disciplinary or ethics codes or standards are violated must be clearly spelled out.

Some departments have introduced special disciplinary procedures for cases of corruption - for example, to allow for speedier processes, for specially trained investigators, and for specially trained and dedicated chairpersons to chair disciplinary hearings. Departments consider such special procedures necessary because many incidents of corruption are high profile cases or cases with the potential to cause great damage and loss to the department (including to its reputation).

KEY REQUIREMENTS FOR SUCCESSFUL DISCIPLINARY ACTION

- **Immediate disciplinary action** must be taken as soon as any irregularity is discovered. Failure to do so creates the impression that management does not view these in a serious light and does not regard them as important enough to deal with immediately. Unnecessary delays can seriously harm the organisation’s image.

- Discipline must be applied in a **consistent, unbiased and fair manner**. If the perception is created that discipline is dealt out in a biased or unfair manner, it undermines its power to deter irregular behaviour. If the impression is created that discipline is not for senior or specially favoured employees, it becomes increasingly difficult to operate the system effectively. For example, staff will become unwilling to report irregularities, to act as witnesses, and to support the organisation’s ethics and anti-corruption drive. It also seriously harms the morale of employees and destroys the trust that staff have in management.

- Cases should be handled with absolute *procedural correctness*. Adhere to all policies and procedures that specify how to go about disciplinary action. This will prevent cases being unresolved due to a procedural technicality not being met.

- It is also important not to get involved in cases which, on the basis of available evidence, have little chance of success. People should not be put through disciplinary action when there is no evidence against them.

Disciplinary procedures are only as good as the people involved. As a result, many organisations put together a pool of staff members who are competent to chair disciplinary proceedings of a serious nature. These people are usually given additional training on the process and their role within the anti-corruption strategy.

The person who presents the case on behalf of the employer must also be trained, competent and informed on the specifics of each case. This usually requires a good relationship between the investigations and disciplinary components to co-ordinate their efforts.

The capacity of both chairpersons and prosecutors can be enhanced through shared service arrangements. The policy below illustrates such an arrangement at the provincial level.

practice

Policy Extract of the Limpopo Provincial Government Anti-Corruption Strategy

Improved prosecution and adjudication capacity on acts of corruption.

In most instances where senior officials are involved in corporate misdeeds and/or officials involved in serious acts of corruption the **action taken against such officials is not commensurate with the incident**. Inconsistencies pertaining to action taken against perpetrators also create a serious crisis of confidence in the government. Prosecution and adjudication capacity will be improved by:

a. Establishing a central prosecution and adjudication pool consisting of qualified and experienced officers charged with the responsibility of prosecuting and adjudicating on corruption cases in the Provincial Government is critical to the fight against corruption.

b. The prosecution and adjudication pool members shall be appointed in writing from various departments by the Director General. Appointed officers will complete appointment forms (attached to the policy as an annexure). Only employees employed on a full-time capacity, as the case may be, may be appointed.

c. The pool shall be coordinated and monitored by the Integrity Management Unit (IMU)

d. Accounting Officers of departments will be advised on appointment of pool members on investigated cases concerning their departments by the IMU

e. The IMU shall as a permanent solution to consistency and efficiency on adjudication and prosecution establish the adjudication and prosecution unit within the IMU.

f. The Director General shall decide on the number of officials who should constitute the pool.

Control over members of the adjudication and prosecution pool

a. The Accounting Officers shall:

(i) Exempt members of the pool of service to attend such training and meetings as made known from time to time.

(ii) Exempt pool members of his or her normal duties to enable him or her to exercise his rights.

b. The Integrity Monitoring Unit shall :-

(i) Make arrangements for exempting members of the pool of their normal duties to enable them to attend to matters of adjudication and prosecution.

Although there are great benefits to having a dedicated pool of chairpersons, there is a risk that you should guard against, and that is that they might become a target for corruptors who want to influence the outcomes of disciplinary processes.

further reading

The Public Service Commission has published the following guidelines:

- Guidelines to follow when considering the merits of an appeal in a case of misconduct
- Guidelines on the management of suspensions

www **www.psc.gov.za/docs/guidelines/main.html**

6.2. *Improving controls and prevention measures*

Once corruption has been uncovered, internal controls and other prevention measures must be reviewed to see whether any weaknesses in this area contributed to the incident. The investigative component should always make recommendations on improving these in their reports. It is also good practice to work with the line management of the function where the incident took place to determine workable solutions, since they will be responsible for implementing any recommendations.

critical link

When considering what can be done to improve controls, have a look at Chapter 3 – Preventing corruption. For example, an immediate and focused training session could be held for people in the functional area involved.

resolution
investigation
detection
prevention

6.3. *Referring cases to other agencies*

MACC

"Each accounting officer must establish a capacity to refer allegations of corruption to a relevant law enforcement agency or other appropriate agencies/ bodies in terms of a formal arrangement."

Many national agencies (likes the SAPS, the Special Investigating Unit and the Auditor-General) play important roles in the national fight against corruption. Although **all** cases of corruption must be referred to law enforcement agencies (SAPS or the Scorpions) for prosecution, many other agencies play a role and can provide assistance – as set out in the following table.

Agency	Functions	When to use them
SAPS	Investigation of all criminal activity.	Most corruption cases can be referred to SAPS, although very serious cases should be referred to the Scorpions. Section 34 of the Prevention and Combating of Corrupt Activities Act also requires senior managers to refer any cases involving R100 000 or more to SAPS.
Directorate for Special Operations and Serious Economic Offences - (Scorpions)	Falls under the control of the National Prosecuting Authority. The Scorpions deal with organised crime and serious financial crimes (including corruption).	The Scorpions will only deal with: • Sensitive and/or high profile cases. • Corruption involving organised syndicates.
Asset Forfeiture Unit	Falls under the control of the National Prosecuting Authority. The Asset Forfeiture Unit's role is to seize the assets of people associated with organised crime.	The Asset Forfeiture Unit will only get involved if: • They believe they have a real chance of recovering assets. • The department will not be bringing its own civil case for recovery against the people involved.
State Attorney	Provides a comprehensive, legal service to the National Government, Provincial Governments, other state funded bodies and their employees.	When the department wants to institute a civil claim to recover losses. The State Attorney cannot be used if you are going to use the Asset Forfeiture Unit.

Agency	Functions	When to use them
Special Investigating Unit (SIU)	• Investigate corruption, serious maladministration, improper conduct and unlawful expenditure of public money or property within state institutions. • Deal with civil recovery of assets and money owed to state institutions. • Taking action to prevent losses to State assets and money • Refer evidence of criminal conduct to the prosecuting authorities. • Advise State institutions on disciplinary action.	The SIU has wide powers to investigate a whole range of crimes, including corruption and fraud and offer advice to departments on disciplinary action. Departments can refer any cases of corruption, maladministration and so on to this Unit to investigate. The SIU will either use an existing Proclamation from the President, or obtain a new one if necessary, that will set out their powers If the investigation shows that corruption has taken place, the SIU will refer it to the National Prosecuting Authority for prosecution, or the President can set up a Special Tribunal to hear the matter.
Public Protectors Office	This Office investigates any improper conduct in the public administration (or conduct that leads to prejudice). While they may recommend people be prosecuted, they do not prosecute anyone themselves.	Departments, individual staff members and members of the public can report cases involving the abuse of power, dishonesty, unfair conduct or improper enrichment with respect to public money directly to this Office.
Auditor-General	The Auditor-General conducts auditing in organisations – including forensic auditing - to assist in the prevention, detection and investigation of economic crimes.	Departments can request the Auditor-General to assist in any cases of corruption involving money.
National Intelligence Agency (NIA)	The NIA is responsible for providing Government with domestic intelligence and counter intelligence.	Highly sensitive cases that impact negatively on good governance, service delivery and stability should be referred to the NIA, which will investigate the case and may then decide to refer it for prosecution.
Public Service Commission (PSC)	The PSC is responsible for investigating and evaluating staff and public administration practices in the public service.	Departments should refer cases to the PSC whenever the Public Service Regulations have been transgressed. Of course, corruption cases must **also** be referred to SAPS or the Scorpions for prosecution.
Department of Public Service and Administration (**dpsa**)	The **dpsa** formulates policies, regulations and frameworks to support effective anti-corruption work.	The **dpsa** can be approached for advice and information on referral agencies, but they do not investigate or prosecute cases themselves.

It is also possible for departments to use the criminal justice system to recover their losses, particularly in less serious offences or those involving smaller losses where a suspended sentence is appropriate. Section 297 of the Criminal Procedure Act (51 of 1997) allows a court hearing a criminal case to order that the accused compensates the victim (the department) for the loss they suffered as a condition of their suspended sentence. For example, the court could sentence someone to six months imprisonment and then suspend this on condition that they repay the money within three months – if they don't, they go to jail.

The easiest way of doing this is simply to ask the prosecutor to request the court to order the accused to repay the money as part of their sentence (if, of course, the person is convicted). In this way, the person is punished for their action (they have a criminal conviction and a suspended sentence hanging over them) **and** the department gets back what it lost without having to go through an expensive civil trial.

Departments should have a clear policy regarding who decides which external agencies to refer matters to and at which point. For example, it might be necessary to ask for the assistance of the SIU early on in the investigation or it might be so clear that corruption has taken place that a case can be referred to SAPS without conducting an investigation. Where a department has a dedicated anti-corruption function, this is usually their responsibility. Whoever is authorised to make such decisions must have the necessary competence and should be in close contact with all the agencies mentioned so that they know which to turn to. It is also good practice to formalise the department's relationship with the SIU, the SAPS, the Scorpions and, if appropriate, the NIA so that, if the person responsible for dealing with these cases leaves, the relationships continue. It will also ensure that departments are kept informed of the progress of their cases.

Note:

People responsible for referring cases to other agencies must have a clear understanding of what these do so that they can choose which one to use. They should **not** refer the same case to various agencies, since this leads to duplication and waste of resources.

practice

Example: The Integrity Management Unit (IMU) in the Limpopo Office of the Premier

The Integrity Management Unit (IMU) in the Limpopo Office of the Premier plays a key role in coordinating the provincial anti-corruption strategy. The IMU is responsible for coordinating with all departments and institutions that have an anti-corruption function in the province to align their efforts. To achieve this, they have set up a Corruption Coordinating Committee in the province which includes:

- National Prosecuting Authority, especially the Scorpions
- Special Investigation Units (SIU)
- South African Police Services (Commercial Crimes Branch)
- National Intelligence Agency (NIA)

They meet once a month to discuss cases of corruption that they are currently working on, which ensures their efforts are well coordinated.

6.4. Feeding information into the organisation's corruption database

Cases of corruption must be entered in the corruption database, which must be regularly updated throughout the process of investigating and resolving cases. Once a case has been resolved (both internally and externally), the outcomes and recommendations must be entered into the database. These cases can then be marked as 'Resolved', but they should be kept on the system for record keeping and trend analysis.

critical link

Information on case and outcomes must be forwarded to the **dpsa** on an annual basis (see page 60).

7. Bringing it all together

Sample Progress Report - a checklist to track progress

The following progress report can be used as a checklist by departments to make sure they have the necessary capacity in all anti-corruption areas:

	Required action steps	Yes	No	In Process
1	Has a meeting(s) been arranged with all stakeholders to address the need for a special ethics and/or anti-corruption drive?			
2	Have these meetings identified the key VALUES to underpin all the department's future actions?			
3	Has an "ethics champion" been identified?			
4	Has an ethical risk survey been done?			
5	Has the information from the risk survey been reported to the relevant decision-makers?			
6	Has any existing ethical or anti-corruption capacity been assessed?			
7	Has a comprehensive ethics or anti-corruption strategy been compiled?			
8	Has an official code of conduct (ideally a clearly focused ethical code) been compiled?			
9	Have specific and detailed action plans been drawn up to implement the anti-corruption strategy?			
10	Have dedicated structures been identified to take responsibility for the different functions identified in the detailed action plans?			
11	Have specific roles, functions, duties, tasks and responsibilities been clearly allocated and formalised?			
12	Have the existing policies, systems and procedures been reviewed for possible improvement in terms of identified risks?			
13	Has an awareness campaign and cultural change programme been implemented?			
14	Have communication channels been identified or put in place to communicate all ethics and anti-corruption information to employees?			
15	Have comprehensive training programmes been launched to support the initiatives?			

	Required action steps	Yes	No	In Process
16	**Are proper reporting mechanisms in place?**			
17	**Are employees fully informed about how these reporting mechanisms function?**			
18	**Are policies and systems in place to investigate irregularities?**			
19	**Are policies and systems in place to refer cases to external authorities, when appropriate?**			
20	**Have disciplinary procedures been reviewed to align these to the anti-corruption strategy?**			
21	**Has a secure and reliable data base been established to capture reports?**			
22	**Is the department's performance in terms of ethics and corruption monitored and regularly reported to all stakeholders and all decision-makers?**			

Examples from practice: Shared wisdom from various Departments:

- Adequate capacity is an absolute prerequisite
- Legal capacity is especially valuable
- Expertise should be sourced from outside if there is insufficient internal capacity
- A zero tolerance stance is the only solution. Even small transgressions need to be addressed (for example: late-coming and abuse of sick leave)
- Irregularities have to be addressed with a real sense of urgency
- Cases should only be pursued if sufficient evidence is available to secure positive outcomes (although it is usually up to the police to decide whether or not they think they have enough evidence to prosecute the case)
- Absolute procedural correctness is required in all cases
- All cases need to be followed up and finally resolved
- Proper checks and balances need to be put in place (for example: a referral to another authority needs to be counter-signed by more than one person)
- Proper paper trails must be secured

8. Conclusion

This booklet is quite technical and shows how the ‘engine’ to fight corruption works. Perhaps of even greater importance is the fuel that drives this engine - the **will** to fight corruption and to create a healthy, ethical, and prosperous South Africa. The requirements, recommendations and case studies in this booklet reflect the progress of the journey towards such a South Africa and we appreciate and respect those who have brought us this far. We invite all departments and individuals to join us in adding further momentum to this journey.

9. Additional resources

further reading

Web-space has been allocated to support this booklet.

There you will find:

- A .pdf version of the booklet
- All the legislation referred to in the booklet
- Sample policies from various departments
- A list of accredited training institutions

www **www.dpsa.gov.za/macc/**

The following international websites can also be visited for an indication of practices in other countries:

Independent Commission Against Corruption

- www.icac.nsw.gov.au

Transparency International

- www.transparency.org

Organisation for Economic Co-operation and Development

- www.oecd.org

South Africa has also ratified the following international anti-corruption initiatives.

UN Convention Against Corruption

- www.odccp.org/odccp/crime_cicp_convention_corruption_docs.html

AU Convention on Preventing and Combating Corruption

- www.africa-union.org

SADC Protocol Against Corruption

- www.sadc.org

References

Asian Organisation of Supreme Audit Institutions. *Understanding Fraud and Corruption*. http://www.asosai.org/guidelines/guide_un_st_fru_corruption.htm (Accessed 15 November 2005)

Klitgaard, R. 1988. *Controlling Corruption.* Berkeley: University of California Press.

Levin, R, Mafunisa, J and Painter-Morland, M. *Corruption Prevention.* Pretoria: University of Pretoria and the Public Service Commission

National Treasury: Office of the Accountant General. *Final Risk Management Framework for the Public Sector.* http://oag.treasury.gov.za/ (Accessed 1 November 2005)

New South Wales Treasury: Office of Financial Management. 1997. Risk management and Internal Controls Toolkit. http://www.treasury.nsw.gov.au/indexes/pubs_by_pol.htm (Accessed 1 November 2005)

New York State: Division of the Budget. *Financial Terminology.* www.budget.state.ny.us/citizen/financial/audit.html (Accessed 27 October 2005)

Schwartz, S. 2004. *Glossary of financial terms*. www.rivernetwork.org/library/Accounting-GlossaryofTerms.htm (Accessed 27 October 2005)

South Africa. Department for Public Service Administration. *Guideline Booklet for implementing requirements to establish minimum anti-corruption capacity in all departments and organisational components in the public service*. Pretoria: dpsa

Standards Australia International. 2003. *AS 8001-2003 – Fraud and Corruption Control.* Sydney: Standards Australia International Ltd.

Steinberg, S.S. & Austern, D.T. 1990. *Government, Ethics, and Managers A Guide to Solving Ethical Dilemmas in the Public Sector.* Westport, CT: Praeger Publishers

Thanks

The **dpsa** wishes to thank the following departments for their generous support in sharing their good practice for the purpose of this booklet:

- Department of Correctional Services
- Department of Public Works
- Department of Trade and Industry
- Independent Complaints Directorate
- Gauteng Shared Services
- Kwa-Zulu Natal Treasury
- National Treasury
- Office of the Premier - Limpopo
- South African National Defence Force
- South African Police Service

This guide was developed with professional support from:

- The University of Pretoria, Centre for Business and Professional Ethics
  - Tel: +27 (0)12 420 4373
- Greg Moran and Associates.
  - Tel: +27 (0)11 880 9940

This publication was made possible through generous support from the German Technical Co-Operation (GTZ)

gtz Partner for the Future. Worldwide.

This publication was made possible through generous support from the German Technical Co-Operation (GTZ)