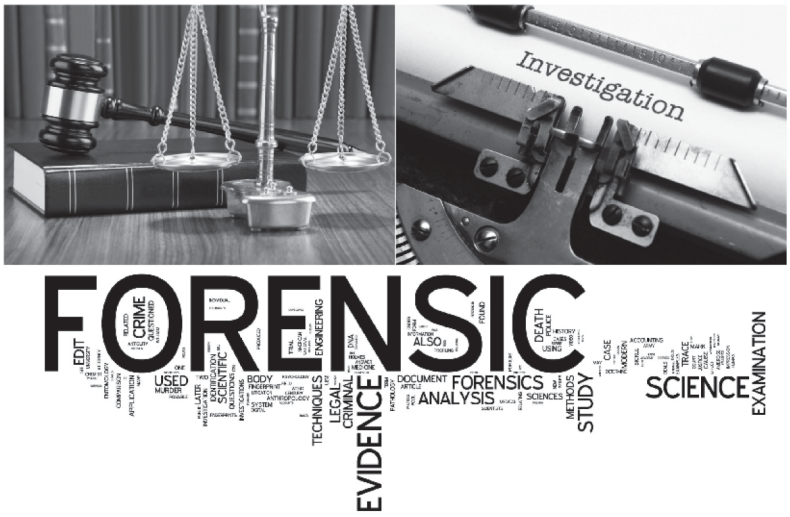
FORENSIC METHODS AND TECHNIQUES II: MODULE A

Only Study guide for **FOR2601**



Dr Setlhomamaru Dintwe

With contributions from:
Mr Stefan Grobler
Mr Andre Botha

DEPARTMENT OF POLICE PRACTICE
UNIVERSITY OF SOUTH AFRICA, PRETORIA

Printed and published
by the University of South Africa
Muckleneuk, Pretoria

FOR2601/1/2016-2018

60162600

Shutterstock.com images used

Editor and Styler

PUB_Style

Contents

PREFACE

Welcome to yet another exciting year of study. I sincerely hope that your studies will be enjoyable and rewarding this year and that you will be able to apply the methods and techniques described in this module with great success.

This module will deal with the methods and techniques relating to forensic investigation. It is intended to give you an understanding of the various approaches that can be employed during an investigation. Many of the concepts sound similar and may cause confusion because they are often used as synonyms, although they have different meanings. For example, consider the words "identify" and "individualise". These words cause tremendous confusion – even among experienced investigators, who often use them incorrectly. Remember that it is vitally important in the investigation of crime and transgressions that you communicate with a third party in clear and understandable language. By "third party", I am referring to a prosecutor or another person who is not directly involved in the investigation, but who has to make a decision based on the contents of your report or case docket.

At the end of this module you will find a glossary of terms. It contains mostly Latin words that are used in the legal environment. These explanations will enable you to understand what they mean in the context in which they occur. Of course, you need not learn these terms off by heart; you just need to be familiar with them and how they are used.

Don't become discouraged if you do not immediately grasp the meaning of a word or a concept. Like all areas of specialisation, forensic investigation has its own unique terminology and you will need to understand what it means if you are to communicate effectively with others.

Please do not rely solely on this module as a source of information. You must also do independent reading and research, as well as speaking to senior, experienced investigators.

Bear in mind that there is a lot of repetition in this module for good reason. I want to keep you focused and prevent you from having to page around looking for explanations.

As much as I have relied on the latest publications in compiling this module, I have also relied on older literature that contains relevant explanations.

PART 1

The work environment for forensic investigation

Contents

Chapter 1

The parameters of the forensic investigation milieu

Contents

1.1 INTRODUCTION

The aim or purpose of this chapter is to give you some background information on the methods and techniques employed by investigators to solve crimes and transgressions, or – as it is referred to in forensic investigation – to resolve the issue at hand.

As this chapter unfolds, you will gain insight into these methods and techniques and see how they are used and which legal requirements govern the various processes. Since the law is constantly changing, some of you may feel that the Judges' Rules have no place in the modern investigative environment. However, these rules are of great value because they help to protect the rights of a suspected or arrested person.

This chapter has been written with practical application in mind and I have grouped the concepts together logically. You will also find a number of activities, which you are urged to do, so that you are able to understand the concepts and apply them in practice.

1.2 DEFINITION OF CONCEPTS

I will begin this chapter by laying a foundation for your understanding by defining the essential concepts in this module.

1.2.1 Forensic

The word "forensic" is used in many different forms and sounds very academic, whereas, in fact, it simply means "for judicial or court purposes". The word is derived from the Latin word *forensis,* which means "forum" or "court". It therefore means "belonging to courts of justice or to public discussion and debate" (*Webster's dictionary* 1942:293).

The *Collins pocket English dictionary* describes the term as being derived from the Latin word *forum,* meaning a "market place" suitable for a law court (1986:333).

When we refer to a "**forensic investigation**", we mean that the investigation has the purpose of ending up in court. A "**forensic investigator**" is a person who does an investigation with the intention of taking the matter to a court, where guilt or responsibility will be determined.

Please note that the forensic investigator is not the person who finds a person guilty. His or her job is only to apply the correct forensic methods and techniques in such a manner that the presiding authority will convict or acquit the person. Your job, therefore, is not to prejudge a person, but to conduct an objective investigation and to remain neutral.

For the same reason, a "**forensic audit**" means that an investigation is undertaken with the intention of determining who was responsible for the misappropriation or mismanagement of money so that he/she may be found guilty, be required to repay the money and even face a prison sentence of some sort.

Investigators have varying powers, depending on the environment in which they operate. Police investigators operate in terms of the provisions of the common law, as well as various statutory provisions. Other investigators may have other powers. Sometimes they may be referred to as "inspectors", but they have certain powers that are bestowed on them by the particular laws under which they operate.

1.2.2 Method

Webster's dictionary describes this term as "a way or mode by which we proceed to the attainment of some aim"; “systematic or orderly procedure".

The *Collins pocket English dictionary* (1986:527) defines this term as "a way of doing anything, especially a regular, orderly procedure".

The word is derived from the Greek words *meta* (after) + *hodos* (a way) (*Collins* 1986:527).

After studying various definitions given on the internet, I suggest the following definition: "Method is a body of techniques for investigating phenomena by acquiring new knowledge or correcting and integrating previous knowledge by gathering information through observation and the formulation of hypotheses" (http://en.wikipedia.org./wiki/Scientific_method).

This is done through the use of experience to find an explanation for what has happened and to make a deduction, based on the possibilities that were formulated. From this, it is clear that the word refers to the **way** of doing something or to **what** to do.

1.2.3 Technique

The internet defines this term as "a systematic procedure used to accomplish a specific activity or task" (http://en. wikipedia. org./wiki/Technique). *Webster's dictionary* describes technique as an "expert method of execution or manner of performance … one skilled in any technical art" (1942:742). The *Collins pocket English dictionary* (1986:866) defines it as "the method of procedure in artistic work, scientific operation etc". The word is derived from the Greek word *techne,* which means ‘an art’.

I prefer the internet definition because it supports the concept of criminal investigation, which is a systematic search for the truth. From this, it is clear that the word refers to **how** something is done.

If you turn once again to the example given above, you will immediately see that merely doing the right thing does not necessarily guarantee success. You have to do the right things **right** (i.e. correctly). Say, for instance, you have traced a suspect and you wish to ask him/her some questions. You know that you must warn him/her, but you cannot remember exactly how to do so, so you just tell him/her to be careful about what he/she says. You have done the right thing by warning him/her, but the way in which you issued the warning is not right (i.e. it is incorrect). You have to observe the Judges' Rules and the suspect’s constitutional rights; only then will you have you done the right thing right (i.e. correctly). The secret of success in an investigation is in **how** you obtain the evidence. If you obtained it legally and it is relevant, there is no reason why it should not be accepted as proof in court.

1.2.4 Forensic tactics

In order to understand the concept of tactics, it is a good idea to differentiate between the words "tactic" and "tact".

1.2.4.1 Tactic

The *Pocket Oxford dictionary* describes "tactic" as "the art of disposing troops or warships especially for or in battle".

The internet describes it as "a conceptual action to achieve a specific objective" (http://en. wikipedia.org/Tactic).

Therefore, "tactic" refers to the actions or the procedures that are followed in the forensic investigation process. If you consider what SWAT teams do in police organisations throughout the

world, it should help you to see that tactics are the actions that these teams use to overcome a specific threat.

1.2.4.2 Tact

You may wonder why I am discussing two similar sounding concepts. Although the words sound similar, they have very different meanings. As you learnt above, "tactic" is the action of doing something, whereas "tact" is the skillful way in which a difficult situation is dealt with (Oxford 1960:851). It refers to the diplomatic way in which a situation is dealt with – avoiding confrontation and obtaining cooperation from an aggressive person.

The internet describes tact as "the acute sensitivity to what is proper and appropriate in dealing with others including the ability to speak or act without offending" (http://www.thefreedictionary.com/tact).

In many instances, suspects refuse to accept guilt or their part in having done something wrong. When the concept of tact is discussed below, the importance of getting a suspect to accept responsibility for their wrongdoing will become evident. It is not about getting a person to admit guilt, but rather to accept responsibility, because there are many reasons why people do something that, on the face of it, appears to be a crime or a transgression.

Investigation is an art. It is about outwitting or outsmarting the transgressor and achieving success in the investigation by applying the correct and legally acceptable methods and techniques.

You must remember that the suspect will almost always deny guilt or involvement in the matter. A suspect will usually attempt to justify his or her actions, or shift the blame to someone else. It is only in exceptional cases that a person will come forward voluntarily and admit to having committed a crime or transgression. People usually only offer to repay or make good the damage that they have caused because they have been caught out or something has happened to make them come forward. This is usually only to try and escape prosecution or lessen the punishment that they may receive. Experience has shown that this kind of behaviour is often the result of fear of some kind, to get rid of a competitor, or to "get even" with another person for some actual or perceived injustice.

As much as the investigator will adopt certain tactics in investigating the matter, so will the suspect to avoid detection or to thwart the investigation. It is for this reason that you have to be aware of all the pitfalls and dangers that await you and take steps to avoid them. These will be discussed later on.

SCENARIO

Let's now apply these concepts in practice. Assume that you are a forensic investigator. You have been tasked to investigate an allegation that an employee of a company has taken a bribe to allow a person who submitted a tender for a large contract to see the tenders that were submitted by other bidders, thus enabling him to submit a lower quote and thereby win the contract.

ACTIVITY 1.1

This activity is aimed at testing whether you understand the concepts that I have just discussed. Reread the scenario and then answer the following questions:

1. What technique would you use to plan your investigation?
2. What tactic would you use to obtain evidence?
3. What method would you use to start the investigation and protect and preserve evidence?

4. How would you use tact to obtain evidence from an uncooperative witness?

You may have noticed that I have intentionally used the five most important questions to ask when doing an investigation. These are largely contained in the so-called five- questions rule that was discussed in FOR1501, namely **what**, **where**, **when**, **who** and **how**. By asking yourself these questions, you will already have started with the tactical approach. The technique is referred to in the last question, namely **how**. If you apply these questions to the scenario, you will get an idea of the approach and the special efforts that you will have to use to attain success.

1.3 THE WORK ENVIRONMENT IN THE FIELD OF CORPORATE, PRIVATE AND PUBLIC SERVICE LAW ENFORCEMENT AGENCIES

The environment in which the forensic investigator works depends on the legal powers bestowed on him/her. To give a practical example, corporate investigators derive the power to do their work from the policies and procedures of the company that employs them. As soon as those persons leave the employ of the company, the rights and powers that they have fall away and they become ordinary citizens.

When employees join a company, they subject themselves to the disciplinary policies and procedures of the organisation. This is done when they sign the employment contract. That is why the management of a company has the right to act against an individual employee whose transgression affects the work of the company.

This is where the task of corporate investigators starts. They are employed to investigate the allegations and to submit a report on their findings to the human resource manager, who is usually a member of the disciplinary committee. The task of the disciplinary committee is to consider the report and to decide on appropriate steps to be taken. I will examine this subject in greater detail later on.

Private investigators, on the other hand, have no rights or powers on which to rely when they conduct an investigation, unless they have been specifically mandated by their client. Their powers are the same as those of a private person and they need to take careful note of the laws that protect an individual's right to privacy. Such investigators need to be aware of the dangers and pitfalls that are present when doing investigations that fall outside the protection of the law.

There are various categories of public service law enforcement officials, which I will elaborate on in due course. For now, it is important to note that not all public service law enforcement officials enjoy the same rights and powers. However, all are bound by the parameters of the laws under which they have been appointed and in terms of which they operate. There are numerous agencies of this nature and although I will not discuss all of them, I will deal with the basic elements/characteristics that are common to all.

1.3.1 Corporate investigators

The term "corporate" refers to a group. In this module, however, the concept refers to a company or an organisation that has been set up in terms of the provisions of the Companies Act 61 of 1973, or to a public entity referred to in section 1 of the Public Finance Management Act 1 of 1999 (hereafter referred to as the "PFMA"). An example is Eskom, which is a major public entity, which has its own corporate investigators. Please note that when you consult the PFMA, it is also important to consult the Public Finance Management Amendment Act 29 of 1999, as well as the Municipal Finance Management Act 56 of 2003, which has similar provisions.

1.3.2 Public entities

Public entities also mean national public entities and refer to –

(a) a national government business enterprise; or
(b) a board, commission, company, corporation, fund, or other entity (other than an national government business enterprise) which is –
    (i) established in terms of national legislation;
    (ii) fully or substantially funded either from the National Revenue Fund, or by way of a tax, levy or other money imposed in terms of national legislation; and
    (iii) accountable to Parliament s 1 of Public Finance Management Act 1 of 1999).

To give you an idea of the different work environments in which corporate investigators may operate, I will list the various public entities that exist in South Africa. There are no less than 20 such public entities, which are divided into the following categories:

- Agencies – National Intelligence Agency (NIA)
- Associations – South African Local Government Association (SALGA)
- Authorities – The South African Police Service (SAPS)
- Boards – The Financial Services Board (FSB)
- Bureaus – The South African Bureau of Standards (SABS)
- Commissions – The Commission for Conciliation Mediation and Arbitration (CCMA)
- Companies – The Electricity Supply Commission(Eskom)
- Corporations – Armscor
- Councils – The Council for Scientific and Industrial Research (CSIR)
- Enterprises – Metrorail
- Foundations – National Research Foundation (NRF)
- Funds – The Road Accident Fund (RAF)
- Institutes – Institute for Public Finance and Auditing (IPFA)
- Institutions – The South African Reserve Bank (SARB)
- Organisations – The National Gambling Board (NGB)
- Regulators – The National Electricity Regulator of South Africa (NERSA)
- Schemes – The National Student Financial Aid Scheme (NASFAS)
- SETAs – Sectoral Education Training Authority (SETA)
- Tribunals – Competition Tribunal
- Trusts – Independent Development Trust (IDT)

If you look at Schedules 1, 2 and 3 of the PFMA, you will see that these entities have been divided into groups. **Schedule 1** refers to constitutional institutions, **Schedule 2** refers to major public entities and **Schedule 3,** to other public entities. I will be dealing with an example of each to illustrate the powers that they have and the environment in which they operate.

Public entities are usually overseen by government departments. For instance, the South African Local Government Association (SALGA) is overseen by the Department of Provincial and Local Government, while the Public Protector and the South African Police Service are constitutional entities in their own right.

Apart from the public entities that have been mentioned above, there are also "Other Public Entities", referred to in Schedule 3. There are 292 of these in total, which have been divided into three parts:

Part A – national public entities

Part B – national government business enterprises

Part C – provincial public enterprises

– Eastern Cape
– Free State
– Gauteng
– KwaZulu-Natal
– Limpopo

– Mpumalanga
– Northern Cape
– North West
– Western Cape

It is not the purpose of this module to deal with these public entities in any detail. It is sufficient for you to know that many of the Schedules 1, 2 and 3 public entities have investigative powers. Among the most notable are the following:

- The Public Protector (Schedule 1 – constitutional institution)
- Eskom (Schedule 2 – major public entities)
- The Financial Services Board (Schedule 3 – other public entities)

I will be dealing with their respective powers in more detail a bit later.

Should you need to deal with any issue over which a public entity has control, you are advised to approach the public entity directly for assistance and to determine whether it has an investigative capability. If they do have investigative powers, it is quite obvious that the laws that regulate them will give the investigators in their employ certain powers. These investigators may not have the same powers as members of the police service, but they are able to provide valuable insight into the administrative workings of the entity, in addition to providing specialist assistance that an outsider may require in order to achieve success. It is not possible to deal with all the public entities in this module and you must realise that not all of them have investigative capabilities; in the latter case, you would be assisted by the responsible government department that oversees the public entity.

The importance of doing proper research before embarking upon an investigation cannot be overemphasised. By doing research, I don't mean sitting down and spending hours in a library or on the internet. The five-questions rule, which was dealt with extensively in FOR1501 and referred to in paragraph 2.5 above, serves as the basis for determining the tactical steps that need to be taken when starting an investigation.

The first thing for you to do is to determine what has happened. Ask yourself whether a law has been broken. If so, this is a criminal offence. If a criminal offence has not been committed, it may be either a civil matter where the person has to compensate the victim, or it could be a disciplinary transgression for which the person is to be disciplined. The next step is to determine what assistance you may need to bring the matter to finality. If it means asking for assistance from another investigator in a particular public entity or in another organisation, then by all means do so. If you are unsure of whether the person will – or is allowed to – help you, contact the person and find out. Write an official letter requesting the information or the assistance. Remember that the Promotion of Access to Information Act 2 of 2000 may be used to obtain information. This will be discussed later in the module.

Corporate investigators have extensive investigative powers within the organisation in which they operate. They are able to gain access to information that would not be available to external persons – as long as it is for legitimate purposes. You may find that permission must be obtained from a higher authority, so it is a good idea to study any legislation governing the organisation beforehand so that you create a good impression. I will be dealing with some relevant issues in this regard later on.

To illustrate my point, I would like to mention some public entities that have special powers.

1.3.3 Constitutional institutions and other statutory bodies

Section 181 of the Constitution of the Republic of South Africa, 1996 makes provision for the establishment of certain state institutions to strengthen constitutional democracy in the Republic of South Africa. One of these is the Public Protector. These institutions are independent and subject only to the Constitution and the law. They must be impartial and may not be interfered

with by any person or organ of state. They are accountable to the National Assembly, to whom they must report on their performance and functions at least once a year.

1.3.3.1 The Public Protector

The Public Protector is a Schedule 1 constitutional institution. The Public Protector has the power to investigate any conduct in state affairs or in the public administration in any sphere of government that is alleged or suspected to be improper or to result in any impropriety or prejudice. The powers of the Public Protector are regulated by the Public Protector Act 23 of 1994.

The Public Protector can investigate the following:

- Government at any level. This includes central and provincial government, state departments and local authorities – excluding court decisions.
- Any person performing a public function. This includes any person performing an official duty that affects South Africans, such as state employees, police officials and even electoral officers.
- Corporations or companies where the state is involved. Examples are Eskom and Telkom.
- Statutory councils. Examples are the Human Sciences Research Council (HSRC) or the Council for Scientific and Industrial Research (CSIR).

The Act gives the Public Protector wide powers to investigate complaints, including the power to determine the manner in which an investigation must be conducted. The Public Protector is competent to investigate a matter on his/her own initiative or on receipt of a complaint. In the case of the latter, he/she may conduct a preliminary investigation to determine the merits of the complaint, taking into consideration the circumstances of the case.

The powers include the direction that in which any person must submit an affidavit or affirmed declaration, or the power to subpoena such a person to appear before him/her to give evidence and to produce documents that may be relevant to the investigation. Should it appear during the course of an investigation that such a person is being detrimentally implicated in the matter, the Public Protector is obliged to afford that person an opportunity to respond – either by giving evidence or by questioning the witnesses personally or through a legal representative.

The Public Protector also has the power to enter premises to make enquiries and to seize anything that may have a bearing on the investigation. The seizure of evidence must take place under authorisation of a warrant issued by a magistrate or a judge. Such a warrant has a three-month limited period of validity and may be executed only by day, unless it has been authorised for execution by night, at times that are reasonable in the circumstances. There are also provisions for a search without a warrant, as well as the "no knock" entry. This refers to entry to premises without first audibly demanding access and informing the occupant of the reason for the search, when it is likely that the occupant will destroy valuable evidence.

It is important to note the difference between a warrant issued in terms of the provisions of section 21 of the Criminal Procedure Act 51 of 1977 and section 7A of the Public Protector Act 23 of 1994. There are other Acts that also regulate issues pertaining to search and seizure, which differ significantly from those that investigators with a police background are used to. It is therefore of the utmost importance that you familiarise yourself with the legislation that has a bearing on the particular matter that you are investigating, as well as the particular environment in which you find yourself.

1.3.3.2 Major public entity: Eskom

In terms of Schedule 2 of the PFMA (Public Finance Management Act 1 of 1999), Eskom is a major public entity. In terms of the provisions of the Eskom Conversion Act 13 of 2001, Eskom was converted from a statutory body into a public company as Eskom Holdings Limited, with effect from 1 July 2002. The two-tier governance structure of the Electricity Council and the Management Board was replaced by a board of directors.

The conversion of Eskom provided an ideal opportunity to review Eskom's existing governance structures and to design a more effective and streamlined decision-making process. The transition was accomplished smoothly and the conversion, including the creation of new board committees and the induction of board members, was carried out efficiently. The board of directors is the accounting authority of Eskom in terms of the PFMA. The board is responsible for providing strategic direction and leadership, ensuring good corporate governance and ethics, determining policy, agreeing on performance criteria and delegating the detailed planning and implementation of policy to the executive management committee (EXCO).

The board meets quarterly and monitors management's compliance with policy and its achievements against objectives. A structured approach is followed for delegation, reporting and accountability, which includes reliance on various board committees. The chairman guides and monitors the input and contribution of the directors. The board has approved a board charter that provides guidance to the directors in discharging their duties and responsibilities.

Compliance, not only with the letter, but also with the spirit, of relevant governance codes remains a priority for the organisation. As a state-owned enterprise, Eskom is guided by the principles of the Code of Corporate Practices and Conduct contained in the King Report on Corporate Governance for South Africa 2002 (King II Report), as well as the Protocol on Corporate Governance in the Public Sector 2002. Furthermore, the statutory duties, responsibilities and liabilities imposed on the directors of Eskom by the Companies Act 61 of 1973, as amended, are augmented by those contained in the Public Finance Management Act 1 of 1999, as amended by Act 29 of 1999 (PFMA). (Please note that there is a detailed discussion of the PFMA in chapter 3 of this guide.)

The government of the Republic of South Africa is the sole shareholder of Eskom. The shareholder representative is the Minister of Public Enterprises. In terms of the Treasury Regulations issued in accordance with the PFMA, Eskom must, in consultation with its executive authority (the Minister of Public Enterprises), annually conclude a shareholder compact, documenting the mandated key performance measures and indicators to be attained by Eskom, as agreed between the board of directors (board) and the executive authority.

The compact is not intended to interfere in any way with normal company law principles. The relationship between the shareholder and the board is preserved, as the board is responsible for ensuring that proper internal controls are in place and that Eskom is effectively managed. The compact serves to promote and encourage good governance practices within Eskom by assisting to clarify the respective roles and responsibilities of the board and the shareholder, setting out the circumstances when shareholder approval is required, when the shareholder needs to be consulted, and the remaining areas where the board is duly empowered to direct the organisation. The following are the internet links where you can access relevant legislation and authorities in the context of energy provision:

- **Eskom Conversion Act 13 of 2001** (http://www.gov.za/sites/www.gov.za/files/a13-01_0.pdf)
- **NERSA** (National Energy Regulator of South Africa) (http://www.nersa.org.za)
- **NNR** (National Nuclear Regulator) (http://www.nnr.co.za)

1.3.3.3 Other public entities: the Financial Services Board

The Financial Services Board (FSB) is what is referred to as a Schedule 3 public entity. It was established in terms of the provisions of the Financial Services Board Act 97 of 1990, with the purpose "to provide for the establishment of a board to supervise compliance with laws regulating financial institutions and the provision of financial services; and for matters connected therewith" (long title of the FSB Act 97 of 1990).

List of Acts administered by the Financial Services Board

1. Collective Investment Schemes Control Act 45 of 2002
2. Financial Services Board Act 97 of 1990

3. Financial Advisory and Intermediaries Services Act 37 of 2002 (FAIS Act)
4. Financial Institutions (Protection of Funds) Act 28 of 2001
5. Financial Supervision of the Road Accident Fund Act 8 of 1993
6. Friendly Societies Act 25 of 1956
7. Inspection of Financial Institutions Act 80 of 1998
8. Long-term Insurance Act 52 of 1998
9. Pension Funds Act 24 of 1956
10. Short-term Insurance Act 53 of 1998
11. Supervision of the Financial Institutions Rationalisation Act 32 of 1996
12. The Securities Services Act 36 of 2004

It is clear from the above, as well as from the long title of the Act, that the FSB was created to function within a financial environment. Therefore, it can safely be said that it is a specialised field of investigation that will require specialised training. When an investigator is faced with the investigation of an alleged contravention of any of the above legislation, the most important aspect to bear in mind is the provisions of the particular Act.

Before embarking upon any investigation, it is of the utmost importance that you know exactly which legislation covers the investigation and what powers it gives you. If you act without the legal authority or protection that the legislation affords, you may be guilty of committing an offence yourself.

This means that you should firstly determine exactly what the allegation is and then whether it constitutes an offence in terms of the particular legislation. For example, section 27 of the FSB Act makes offences of the contravention of certain sections and prescribes penalties. These will be discussed in greater detail a bit later.

ACTIVITY 1.2

Read any Act of parliament. See whether there is a section that prescribes offences and penalties. Refer to the sections that are criminalised and make a list of what you think you may need in order to prove the matter in a court of law.

Refer, for instance, to the provisions of the Prevention and Combating of Corrupt Activities Act 12 of 2004. You will see that it makes certain actions criminal offences and also provides for certain penalties.

What would you do if the Act does not make provision for offences and penalties? Do you think that there would be no contravention in that case? Give reasons for your answer.

EXAMPLE

Let's use the scenario that appears before activity 1.1 above. Assume that you have been requested by your manager to investigate the matter, which has been reported to him/her anonymously. All that you have are the notes that the manager made during the conversation. You also have the name of the employee, but not of the successful bidder. You will need to obtain evidence and you have decided that the best way to do so is by searching the employee's office and, possibly, also his/her residence.

In the activity below, you will be asked to establish what power/s you have to do the search. Apart from the Criminal Procedure Act, you must also determine whether there is any other legislation or mechanism that would make it possible for you to obtain the evidence. Don't be bound by legislation alone – think about what alternatives you could you use. If you don't find the answer, read a bit further.

ACTIVITY 1.3

1. Have a look at the provisions of the Criminal Procedure Act 51 of 1977. Which section/s will empower you to search the suspect's home or office (or both) in the following three situations?
   (a) if you are a police official
   (b) if you are a corporate investigator
   (c) if you are a private investigator
2. What are the possibilities and what will you do if you do not have the legal powers in the following three situations?
   (a) if you are a corporate investigator
   (b) if you are a private investigator
   (c) if you are a private citizen

Returning to the concepts we discussed at the beginning of the module, think of how you could obtain the evidence if you do not have the legal power to search a person's office or residence. What are the possibilities and what would you do? You should "think out of the box" because you should consider enlisting the help of persons in the investigative industry that have the legal power to do so. This does **not** mean doing an illegal search; it simply means that if certain powers can be used only if a criminal case has been opened, then you should do so. There are many alternative techniques that can be employed to obtain information. You should always consider the possibilities. But also remember that everything that you do may be scrutinised by a court of law and you will face serious consequences if you do anything illegal or unconstitutional.

1.4 INVESTIGATION PARAMETERS

Private, corporate and public law enforcement investigators are bound by certain rules. These rules may be referred to as the parameters that determine what investigators may and may not do. Investigations are conducted according to rules laid down by procedures, as well as by laws. Procedures include instructions as to how an investigation should be done. These can usually be found in standard operating procedures (SOPs) in corporations or in national instructions in the police. Whatever the name used for these procedures, they are a guide to what must be done during an investigation and, also, what the reporting procedures are.

As far as legislation is concerned, the Criminal Procedure Act 51 of 1977 provides for procedures and related matters in criminal proceedings, whereas private law regulates the relations between individuals in a community. To remain within the boundaries laid down for acceptable and legal investigations, you should know the laws and the regulations that are applicable in a particular situation. For instance, if you fail to observe a requirement laid down for the manner in which you are to deal with a suspected person, you may have violated that person's rights. This could mean that the court is likely to acquit the person on a technical point.

In the next paragraph I will discuss some legislative parameters that are crucial in any investigation, as they deal with the rights of the people who may be under investigation for one reason or another.

1.4.1 Bill of Rights

The provisions of section 35(1) of the Constitution are part of the Bill of Rights and are applicable in all cases when dealing with arrested or detained persons. These provisions are as follows:

> 35(1) Everyone *who is arrested* (I have emphasised the words "who is arrested" to show that it does not refer to suspected persons who have not yet been arrested or whom you have not yet decided to arrest because the person claims that they are innocent.

Suspected persons are dealt with in terms of the provisions of the Judges' Rules, which are discussed below) for allegedly committing an offence, has the right –

(a) to remain silent;
(b) to be informed promptly –
    (i) of the right to remain silent; and
    (ii) of the consequences of not remaining silent;
(c) not to be compelled to make any confession or admission that could be used in evidence against that person;
(d) to be brought before a court as soon as reasonably possible, but not later than –
    (i) 48 hours after the arrest; or
    (ii) the end of the first court day after the expiry of the 48 hours, if the 48 hours expire outside ordinary court hours or on a day which is not an ordinary court day;
(e) at the first court appearance after being arrested, to be charged or to be informed of the reason for the detention to continue, or to be released; and
(f) to be released from detention if the interests of justice permit, subject to reasonable conditions.

I will be dealing with subsection (2) of section 35 in due course, but wish to point out to you here that there are a number of provisions in subsection (1) that complement the Judges' Rules. Therefore, it cannot be said that the Judges' Rules are no longer applicable.

ACTIVITY 1.4

1. When must you inform a person of his/her rights according to the Judges' Rules?
2. When must you inform a person of his/her rights in terms of the Constitution?
3. Must the information given to a person in terms of the Judges' Rules and the Constitution be in writing? Please read through the section before answering this question.

1.4.2 Judges' Rules

The Judges' Rules were laid down many years ago during a judges' conference to give direction and guide police officers in how to act when dealing either with persons suspected of having committed offences or persons who have been arrested. Although there was no constitution in place back then, like there is today, the rights of suspected and arrested persons still had to be protected. The Judges' Rules are as follows:

1. Questions may be put by police officers to persons whom they do not suspect of being concerned in the commission of the crime under investigation, without any CAUTION being administered first.
2. Questions may also be put to a person whom it has been decided to arrest or who is under suspicion where it is possible that the person, by his/her answers, may afford information which may tend to establish his/her innocence, for instance where he/she has been found in possession of property suspected to have been stolen or an instrument suspected to have been used in the commission of the crime, or where he/she was seen in the vicinity when the crime was committed. IN SUCH A CASE, A CAUTION SHOULD BE ADMINISTERED FIRST.

   Questions intended solely to elicit answers that provide evidence against the suspect should not be put.
3. The wording of the CAUTION to be administered is as follows: "I am a police officer. I am making enquiries (into so and so) and I want to know anything you can tell me about it. It is a serious matter AND I MUST WARN YOU TO BE CAREFUL WHAT YOU SAY."

If there is any special matter that requires an explanation, the officer should add the following words: "You have been found in possession of/you were seen in the vicinity of … and unless you can explain this, I may have to arrest you."

4. Questions should not be put to a person in custody, with the exception of questions put in terms of rule (7).
5. Where a person in custody wishes to volunteer a statement, he/she should be allowed to make it, BUT HE/SHE SHOULD BE CAUTIONED FIRST.
6. A prisoner making a statement before there is time to caution him SHOULD BE CAUTIONED AS SOON AS POSSIBLE.
7. A prisoner making a voluntary statement must not be cross-examined, but questions may be put to him/her solely for the purpose of removing elementary or obvious ambiguities in VOLUNTARY STATEMENTS. For instance, if he/she has mentioned an hour, without saying whether it was morning or evening, or has given a day of the week and a day of the month that are incompatible, or has not made it clear to which individual or place he/she intended to refer in some part of his/her statement, he/she may be questioned sufficiently to clarify the point.
8. The caution to be administered to a person in custody should be to the following effect:
   (a) Where he/she is formally charged – "Do you wish to say anything in answer to the charge? You are not obliged to do so, but whatever you say will be taken down in writing and may be given in evidence."
   (b) Where a prisoner volunteers a statement, other than on a formal charge – "Before you say anything (or, if he/she has already commenced his/her statement, anything further), I must tell you that you are not obliged to do so, but whatever you say will be taken down in writing and may be used in evidence."
9. Any statement made should, whenever possible, be taken down in writing and in the language in which it was made. It should be read over to the person making it, and he/she should be given the opportunity to make any corrections to it, after which he/she should be invited to sign it.
10. When two or more persons are charged with the same offence and a voluntary statement is made by any one of them, the police, if they consider it desirable, may furnish each of the other persons with a copy of such statement, but nothing should be said or done by the police to elicit a response. The police should not read such statement to a person, unless such person is unable to read it and desires that it be read to him/her. If a person furnished with a co-accused's statement desires to make a voluntary statement in reply, the usual caution should be administered (Coetzee 1983:18).

If you study the Judges' Rules, you will realise that they assist you significantly in performing your job effectively. You are urged to compare the Judges' Rules with the Constitutional requirements to see whether they overlap, are conflicting or complement each other. You will thus be able to protect you against the pitfalls of unconstitutional behaviour.

ACTIVITY 1.5

1. Are you permitted to allow one suspect to see the statement of another if they are not charged with the same offence?
2. What would you do if the two suspects are charged with the same offence?

1.4.3 Promotion of Access to Information Act (PAIA) 2 of 2000

In order for you to be able to use the provisions of this legislation (hereafter referred to as "PAIA"), I have quoted those sections that I feel are relevant to you as a forensic investigator. Please read the sections that are relevant to your particular circumstances and note that all public and private bodies have "public officers" whose task it is to deal with the implementation of this Act. When

you find it necessary to obtain information from such a body in terms of the provisions of this Act, you should contact this person to arrange for what you need. You should also be aware that the administrative procedures may differ from one organisation to the next and that an administrative fee will be payable.

There may also be certain forms that have to be completed. When you do find it necessary to apply for information, I suggest that you first contact the organisation telephonically to make sure that you comply with their particular requirements and know whom to contact when you visit their offices; this will help you to avoid having to stand in queues or being sent from one person to another.

1.4.3.1 Definitions in section 4 of the PAIA

In this section, I provide definitions of concepts that are pertinent to forensic investigation, as contained in the PAIA.

"Private body" means –

(a) a natural person who carries or has carried on any trade, business or profession, but only in such capacity;
(b) a partnership which carries or has carried on any trade, business or profession;
(c) any former or existing juristic person, but excludes a public body.

"Public body" means –

(a) any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government; or
(b) any other functionary or institution when –
    (i) exercising a power or performing a duty in terms of the Constitution or a provincial constitution; or
    (ii) exercising a public power or performing a public function in terms of any legislation (Promotion of Access to Information Act 2 of 2000).

1.4.3.2 Relevant sections

For ease of use and a quick reference, I have quoted from relevant sections to help you, as a forensic investigator, to understand and be able to use the Act to obtain information from both public and private bodies. I recommend that you obtain a copy of this Act and study its provisions so that you know which information you are entitled to access, and which you are not.

Section 9 of the PAIA lists the objects of this Act as follows:

(a) to give effect to the constitutional right of access to
    (i) any information held by the State; and
    (ii) any information that is held by another person and that is required for the exercise or protection of any rights;

(b) to give effect to that right—
    (i) subject to justifiable limitations, including, but not limited to, limitations aimed at the reasonable protection of privacy, commercial confidentiality and effective, efficient and good governance; and
    (ii) in a manner which balances that right with any other rights, including the rights in the Bill of Rights in Chapter 2 of the Constitution;

(c) to give effect to the constitutional obligations of the State of promoting a human rights culture and social justice, by including public bodies in the definition of "requester", allowing them, amongst others, to access information from private bodies upon compliance with the four requirements in this Act, including an

additional obligation for certain public bodies in certain instances to act in the public interest;

(d) to establish voluntary and mandatory mechanisms or procedures to give effect to that right in a manner which enables persons to obtain access to records of public and private bodies as swiftly, inexpensively and effortlessly as reasonably possible; and

(e) generally, to promote transparency, accountability and effective governance of all public and private bodies by, including, but not limited to, empowering and educating everyone —

(i) to understand their rights in terms of this Act in order to exercise their rights in relation to public and private bodies;

(ii) to understand the functions and operation of public bodies: and

(iii) to effectively scrutinise, and participate in, decision-making by public bodies that affects their rights.

ACTIVITY 1.6

1. What do you think are the most important objects of the Promotion of Access to Information Act?
2. Do you think that this Act is applicable to law enforcement officials only, or may a private investigator also make use of it?

1.4.3.3 Forms of request

The manner in which requests for information are to be made is regulated by section 18(1), which determines as follows:

(1) A request for access must be made in the prescribed form to the information officer of the public body concerned at his or her address or fax number or electronic mail address.

(2) The form for a request of access prescribed for the purposes of subsection (1) must at least require the requester concerned –

(a) to provide sufficient particulars to enable an official of the public body concerned to identify –

(i) the record or records requested; and

(ii) the requester;

(b) to indicate which applicable form of access referred to in section 29 (2) is required;

(c) to state whether the record concerned is preferred in a particular language;

(d) to specify a postal address or fax number of the requester in the Republic;

(e) if, in addition to a written reply, the requester wishes to be informed of the decision on the request in any other manner, to state that manner and the necessary particulars to be so informed; and

(f) if the request is made on behalf of a person, to submit proof of the capacity in which the requester is making the request, to the reasonable satisfaction of the information officer.

(3)

(a) An individual who because of illiteracy or a disability is unable to make a request for access to a record of a public body in accordance with subsection (1), may make that request orally.

(b) The information officer of that body must reduce that oral request to writing in the prescribed form and provide a copy thereof to the requester.

ACTIVITY 1.7

1. Make a list of the actions you would take to apply for information.
2. What information would you be entitled to?
3. Do you think that information may be denied if you have not complied with the requirements set out in section 18(1) above?

1.4.3.4 Right of access to records of public bodies

The right to access the records of public bodies is provided for in section 11 and the following subsections clarify the process in accessing such records:

(1) A requester must be given access to a record of a public body if –

(a) that requester complies with all the procedural requirements in this Act relating to a request for access to that record; and
(b) access to that record is not refused in terms of any ground for refusal contemplated in Chapter 4 of this Part.

(2) A request contemplated in subsection (1) includes a request for access to a record containing personal information about the requester.

(3) A requester's right of access contemplated in subsection (1) is, subject to this Act, not affected by –

(a) any reasons the requester gives for requesting access; or
(b) the information officer's belief as to what the requester's reasons are for requesting access.

ACTIVITY 1.8

When may access to information of a public body be refused?

Although the Act determines that nothing prevents the giving of access to the records of a public or a private body, there are certain very important exceptions and limitations that you must take note of.

For the private investigator, who does not have legal backing to obtain information, this Act provides a way for him/her to obtain such information, as long as the prescriptions are followed and the prescribed fees are paid. It is very important to note that there are a number of limitations protecting personal information, as well as information held by private bodies that relates to business and trade secrets.

1.4.3.5 Right of access to records of private bodies

The right of access to the records of private bodies is regulated in terms of section 50 of the PAIA and the following subsections are applicable:

(1) A requester must be given access to any record of a private body if –

(a) that record is required for the exercise or protection of any rights;
(b) that person complies with the procedural requirements of this Act relating to a request for access to that record; and
(c) access to that record is not refused in terms of any ground for refusal contemplated in Chapter 4 of this Part.

(2) In addition to the requirements referred to in subsection (1), when a public body referred to in paragraph (a) or (b)(i) of the definition of "public body" in section 1

requests access to a record of a private body for the exercise or protection of any rights other than its rights, it must be acting in the public interest.

(3) A request contemplated in subsection (1) includes a request for access to a record containing personal information about the requester or the person on whose behalf the request is made.

ACTIVITY 1.9

1. When may access to information of private bodies be given?
2. When may access to information of private bodies be refused?

According to section 36(1), subject to subsection (2), the information officer of a public body must refuse a request for access to a record of the body if the record contains –

(a) trade secrets of a third party;
(b) financial, commercial, scientific or technical information, other than trade secrets, of a third party, the disclosure of which would be likely to cause harm to the commercial or financial interests of that third party; or
(c) information supplied in confidence by a third party the disclosure of which could reasonably be expected –
    (i) to put that third party at a disadvantage in contractual or other negotiations; or
    (ii) to prejudice that third party in commercial competition.

Subsection 2 provides that a record may not be refused in terms of subsection (1) in so far as it consists of information –

(a) already publicly available;
(b) about a third party who has consented in terms of section 48 or otherwise in writing to its disclosure to the requester concerned; or
(c) about the results of any product or environmental testing or other investigation supplied by, carried out by or on behalf of a third party and its disclosure would reveal a serious public safety or environmental risk.

Subsection 3 provides that for the purposes of subsection (2)(c), the results of any product or environmental testing or other investigation do not include the results of preliminary testing or other investigation conducted for the purpose of developing methods of testing or other investigation.

1.4.3.6 Mandatory protection of certain confidential information and protection of certain other confidential information of third parties

This is provided for in section 37 of the PAIA. The following excerpts from the Act stipulate the procedure:

(1) Subject to subsection (2), the information officer of a public body –
    (a) must refuse a request for access to a record of the body if the disclosure of the record would constitute an action for breach of a duty of confidence owed to a third party in terms of an agreement; or
    (b) may refuse a request for access to a record of the body if the record consists of information that was supplied in confidence by a third party –
        (i) the disclosure of which could reasonably be expected to prejudice the future supply of similar information, or information from the same source; and

(ii) if it is in the public interest that similar information, or information from the same source, should continue to be supplied.

(2) A record may not be refused in terms of subsection (1) insofar as it consists of information –

(a) already publicly available; or
(b) about the third party concerned that has consented in terms of section 48 or otherwise in writing to its disclosure to the requester concerned.

It is important for you to take note of the provisions of sections 36 and 37, particularly the wording of the sections. Whereas section 36 places a prohibition on the disclosure of certain information, section 37 makes provision for an official to apply discretion.

1.4.3.7 Mandatory protection of privacy of third parties who are natural persons

This situation is regulated in terms of section 34 of the PAIA and the following subsections are applicable:

(1) Subject to subsection (2), the information officer of a public body must refuse a request for access to a record of the body if its disclosure would involve the unreasonable disclosure of personal information about a third party, including a deceased individual.
(2) A record may not be refused in terms of subsection (1) insofar as it consists of information –

(a) about an individual who has consented in terms of section 48 or otherwise in writing to its disclosure to the requester concerned;
(b) that was given to the public body by the individual to whom it relates and the individual was informed by or on behalf of the public body, before it is given, that the information belongs to a class of information that would or might be made available to the public;
(c) already publicly available;
(d) about an individual's physical or mental health, or well-being, who is under the care of the requester and who is –

(i) under the age of 18 years; or

(ii) incapable of understanding the nature of the request, and if giving access would be in the individual's best interests;

(e) about an individual who is deceased and the requester is –

(i) the individual's next of kin: or

(ii) making the request with the written consent of the individual's next of kin; or

(f) about an individual who is or was an official of a public body and which relates to the position or functions of the individual, including, but not limited to –

(i) the fact that the individual is or was an official of that public body;
(ii) the title, work address, work phone number and other similar particulars of the individual;
(iii) the classification, salary scale or remuneration and responsibilities of the position held or services performed by the individual; and

(iv) the name of the individual on a record prepared by the individual in the course of employment.

ACTIVITY 1.10

1. When may information regarding an individual who is a natural person be disclosed by a public body?

2. When must an information officer of a public body refuse access to information regarding an individual who is a natural person?
3. Would it make any difference if an estate were involved?

It is very important that you study the provisions of the Act to determine exactly which information you are entitled to apply for. Please also note that in some instances, although the granting of information is prohibited, there are exceptions. These exceptions are contained in the relevant sections that deal with the particular matter. For example, if you are applying for information on an insolvent deceased estate in terms of the provisions of section 34, the information must be refused, unless the executor has given permission or the final liquidation and distribution account has been approved and the estate wound up.

1.4.3.8 Application of other legislation providing for access

Section 6 of the PAIA provides that nothing in this Act prevents the giving of access to –

(a) a record of a public body in terms of any legislation referred to in Part 1 of the Schedule; or
(b) a record of a private body in terms of any legislation referred to in Part 2 of the Schedule.

1.4.3.9 The PAIA does not apply to records required for criminal or civil proceedings after commencement of proceedings

Section 7 of the PAIA provides that:

(1) This Act does not apply to a record of a public body or a private body if –
   (a) that record is requested for the purpose of criminal or civil proceedings;
   (b) so requested after the commencement of such criminal or civil proceedings, as the case may be; and
   (c) the production of or access to that record for the purpose referred to in paragraph (a) is provided for in any other law.

(2) Any record obtained in a manner that contravenes subsection (1) is not admissible as evidence in the criminal or civil proceedings referred to in that subsection unless the exclusion of such record by the court in question would, in its opinion, be detrimental to the interests of justice.

1.4.3.10 Mandatory protection of police dockets in bail proceedings and protection of law enforcement and legal proceedings

Section 39 provides that:

(1) The information officer of a public body –
   (a) must refuse a request for access to a record of the body if access to that record is prohibited in terms of section 60(14) of the Criminal Procedure Act, 1977 (Act 51 of 1977); or
   (b) may refuse a request for access to a record of the body if –
      (i) the record contains methods, techniques, procedures or guidelines for –
         (aa) the prevention, detection, curtailment or investigation of a contravention or possible contravention of the law: or
         (bb) the prosecution of alleged offenders and the disclosure of those methods, techniques, procedures or guidelines could reasonably be expected to prejudice the effectiveness of those methods, techniques, procedures or guidelines or lead to the circumvention of the law or facilitate the commission of an offence;

(iii) the prosecution of an alleged offender is being prepared or about to commence or pending and the disclosure of the record could reasonably be expected –

(aa) to impede that prosecution: or

(bb) to result in a miscarriage of justice in that prosecution; or

(iii) the disclosure of the record could reasonably be expected –

(aa) to prejudice the investigation of a contravention or possible contravention of the law which is about to commence or is in progress or, if it has been suspended or terminated, is likely to be resumed;

(bb) to reveal, or enable a person to ascertain, the identity of a confidential source of information in relation to the enforcement or administration of the law;

(cc) to result in the intimidation or coercion of a witness or a person who might be or has been called as a witness, in criminal proceedings or other proceedings to enforce the law;

(dd) to facilitate the commission of a contravention of the law, including, but not limited to, subject to subsection (2), escape from lawful detention; or

(ee) to prejudice or impair the fairness of a trial or the impartiality of an adjudication.

(2) A record may not be refused in terms of subsection (1)(b)(iii)(dd) insofar as it consists of information about the general conditions of detention of persons in custody.

(3) (a) If a request for access to a record of a public body must or may be refused in terms of subsection (1)(a) or (b) or could, if it existed, be so refused and the disclosure of the existence or non-existence of the record would be likely to cause the harm contemplated in subsection (1)(a) or (b), the information officer concerned may refuse to confirm or deny the existence or non-existence of the record.

(b) If the information officer so refuses to confirm or deny the existence or non-existence of the record, the notice referred to in section 25(3) must –

(i) state that fact;

(ii) identify the provision of subsection (1)(a) or (b) in terms of which access would have been refused if the record had existed;

(iii) state adequate reasons for the refusal, as required by section 25(3), in so far as they can be given without causing the harm contemplated in any provision of subsection (1) (a) or (b); and

(iv) state that the requester concerned may lodge an internal appeal or an application with a court as the case may be, against the refusal as required by section 25(3) as set out above.

This simply means that if access to information is denied, full reasons for the refusal must be given and the applicant must also be informed of the right to appeal the decision. This may be an administrative process through the relevant department or a legal one through a court of law.

ACTIVITY 1.11

You are the investigator in a sensitive matter in which you have employed certain legal methods which you would not want to be made known. What are the grounds on which an application for access to your case docket could be refused?

1.4.4 Dangers and pitfalls in forensic investigation

Every investigator should be aware of the dangers inherent in an investigation. Therefore, when you embark on an investigation, it is vital that you not only be aware of "the rules of engagement", but also the rights of the persons against whom the investigation is aimed.

Dangers in an investigation include the following:

- interference by the suspect/accused in the investigation by laying counter-charges against the complainant or even the investigator
- the suspect/accused's absconding after being released on bail
- interference with witnesses in the form of intimidation or bribery
- destruction or contamination of exhibits
- corruption of the investigator
- theft of the case docket
- fabrication of evidence
- inadequate resources, resulting in the investigation's being abandoned
- political or official interference from higher authorities
- unobtainable evidence, such as where evidence is located in a foreign country or in an off-shore bank and you cannot gain access to it for various reasons

ACTIVITY 1.12

1. Make a list of possible steps you would take to protect your case docket from being stolen.
2. What would you do if your case docket contained important original documentary evidence and the prosecutor wished to see it?
3. Think of other possible dangers or pitfalls not listed above.

You may be able to avoid some of these dangers, but may, for instance, find yourself powerless to withstand pressure from a superior to hand your investigation over to another person or unit on the pretext that it falls outside your field of expertise and will be better dealt with by them. Although this may be a reasonable request, there is always the danger that there could be an ulterior motive for it.

Pitfalls to be aware of are those rules of procedure that have been laid down either by law or by other means.

1.4.5 Inhibiting factors in obtaining information

Forensic investigators face many problems when attempting to obtain information, not only from private individuals and organisations, but – especially – from financial institutions. Banks and other financial institutions have strict codes of confidentiality and could face severe civil action by a client if these are violated. The only way in which to obtain information from these organisations is through the application of section 205 of the Criminal Procedure Act, which will be dealt with in below.

Whereas police and certain corporate investigators may have legal powers in obtaining information, private investigators have to rely on what is referred to as "contacts" to try and access information that is normally difficult to obtain. They have no legal power to force any person to cooperate with them or to give them any information. This is one of the reasons why they must rely on tact (see paragraph 2.4.2 above).

1.4.6 Legal remedies for obtaining information

Unless you work for an organisation such as the South African Police Service or a similar organisation, such as the Special Investigating Unit, where you have the legal powers to obtain information, you will have to make use of the provisions of the Promotion of Access to Information Act 2 of 2000 to obtain information from various organisations and bodies. Please note, however, that there are limits to what you are able to obtain. This is a very important legislative method for private individuals to obtain information legally where, in the past it was either not accessible or had to be obtained in ways that were not always acceptable (e. g. by infringing the rights of persons). It is for this reason that I have quoted extensively from the Act to outline the processes and procedures in a logical way. You are urged to obtain a copy of this Act and to keep it available for easy reference.

Of course, the police service and other agencies that have legal powers to obtain warrants for search and seizure simply make use of the provisions of the legislation from which they derive their powers.

ACTIVITY 1.13

1. What other legislation, in addition to that mentioned above, is available to assist you to obtain information? (Read further to find the answer.)
2. Do you think that you would be able to ask the police service if you could use their powers to obtain information for you if you were not a police officer?

1.4.7 Civil law

In civil matters, the so-called Anton Piller Order makes it possible to obtain a court order for the right to search premises and seize evidence without prior warning, thereby preventing the destruction of incriminating evidence. Such an order, which is the civil-law equivalent of a search warrant in criminal cases, allows for the necessary force to be used to gain access to premises (as does the Criminal Procedure Act in criminal matters). Without going into detail, the criteria for obtaining an Anton Piller Order are as follows:

- There must be extremely strong prima facie evidence against a respondent.
- The actual or potential damage must be very serious for the applicant.
- Clear evidence must exist that the respondents have in their possession incriminating evidence and that there is a real possibility that they may destroy such material before an *inter partes* (between parties) application can be made (http://en.wikipedia.org/wiki/Anton_Piller_order).

An Anton Piller Order is executed by the sheriff of the magisterial district in which the order has been issued.

1.4.8 The Criminal Procedure Act 51 of 1977

Section 205 of the Criminal Procedure Act 51 of 1977 makes provision for information to be obtained from persons as well as institutions upon application by an attorney general or a public prosecutor.

> **205. Judge, regional court magistrate or magistrate may take evidence as to alleged offence**
>
> (1) A judge of the supreme court, a regional magistrate or a magistrate may, subject to the provisions of subsection 4, upon the request of an attorney-general or a public prosecutor authorized thereto in writing by the attorney-general, require the attendance before him or any other judge, regional court magistrate or magistrate, for examination by the attorney-general or the public prosecutor authorized thereto in writing by the attorney-general, of any person who is likely to give

material or relevant information as to any alleged offence, whether or not it is known by whom the offence was committed: Provided that if such person furnishes that information to the satisfaction of the attorney-general or public prosecutor concerned prior to the date on which he is required to appear before a judge, regional court magistrate or magistrate.

(2) The provisions of sections 162 to 165 inclusive, 179 to 181 inclusive, 187 to 189 inclusive, 191 and 204 shall mutatis mutandis apply with reference to the proceedings under subsection (1).

(3) The examination of any person under subsection (1) may be conducted in private at any place designated by the judge, regional court magistrate or magistrate.

(4) A person required in terms of subsection (1) to appear before a judge, a regional court magistrate or magistrate for examination, and who refuses or fails to give the information contemplated in subsection (1), shall not be sentenced to imprisonment as contemplated on section 189 unless the judge, regional court magistrate or magistrate concerned, as the case may be, is also of the opinion that the furnishing of such information is necessary for the administration of justice or the maintenance of law and order.

ACTIVITY 1.14

You have served a notice in terms of section 205 of the CPA on a person, but he/she fails to appear on the date and time specified. What will you do?

1.4.9 Special Investigating Units and Special Tribunals Act 74 of 1996

The Special Investigating Units and Special Tribunals Act 74 of 1996 provides that the unit may –

(a) through a member require from any person such particulars and information as may be reasonably necessary;

(b) order any person by notice in writing under the hand of the Head of the Special Investigating Unit or a member delegated thereto by him or her, addressed and delivered by a member, a police officer or a sheriff, to appear before it at a time and place specified in the notice and to produce to it specified books, documents or objects in the possession or custody or under the control of any such person: Provided that the notice shall contain the reasons why such person's presence is needed.

(c) through a member of the Special Investigating Unit, administer an oath to or accept an affirmation from any person referred to in paragraph (b), or any person present at the place referred to in paragraph (b), irrespective of whether or not such person has been required under the said paragraph to appear before it, and question him or her under oath or affirmation.

These provisions are applicable only to members of the SIU and may only be used once the SIU is engaged in an investigation sanctioned by proclamation in the Government Gazette. It is important to note the difference here, as members of the SA Police Service may use the provisions of section 205 of the Criminal Procedure Act only once a criminal investigation is underway.

ACTIVITY 1.15

What do you think are the main differences between a subpoena in terms of section 205 of the CPA and section 5(2)(b) of the SIU Act?

1.5 SUMMARY AND CONCUSION

Investigators worldwide encounter problems relating to obtaining evidence. They require such evidence to prove the guilt – or innocence – of a person. In the process, they have to use many techniques and tactics to obtain the information that they seek.

Not all investigators have access to legislation that allows them to obtain the information they seek; consequently, they have to rely on cumbersome methods that sometimes fail to provide the desired outcome. Those investigators that do have the backing of legislation and official powers to perform their work must do so in strict accordance with the legislation. If they go beyond what the legislation allows, it will affect their credibility and may even destroy the investigation in which they have invested so much time.

It is vitally important that investigators know not only the law and the particular rules regarding an investigation, but also how to report on their findings in such a way that the recipient is able to make an informed decision. The information contained in a report must have been obtained through a legal and transparent process. This involves not only questioning and interrogation, but also the use of recording apparatus such as recorders and other devices used to capture and store images and voice recordings.

We are living in times when the law is continually changing as a result of new decisions handed down by the courts. Investigators should take notice of such changes and keep abreast of new legislation, otherwise they run the risk of being left behind.

Chapter 2

Professional conduct for forensic investigators

Contents

2.1 INTRODUCTION

A code of professional conduct is a necessary component of any profession in order to maintain standards for the individuals working within that profession. Such a code ensures accountability, responsibility and trustworthiness on the part of the individuals affiliated with that profession.

While a police investigator deals not only with persons who are victims of crime, but also with persons who are witnesses in criminal matters, private and corporate investigators deal mainly with disciplinary or civil matters. Victims of crime usually cooperate with the police investigator because they have a vested interest in the matter and they wish to see the perpetrator prosecuted and sentenced. Witnesses, on the other hand, are sometimes reluctant to cooperate with the police because they fear reprisals from the suspect or simply do not wish to become involved. In the investigation process, the SAPS investigator has legal powers (as discussed in chapter 1) to compel witnesses – and potential witnesses – to cooperate and provide the information needed to prove a case. Therefore, the witness has very little choice and is compelled to cooperate with the police to avoid breaking the law. Because police investigators know that they have this power, they often treat witnesses with less respect than they deserve.

The private investigator, on the other hand, does not have these powers and must rely on the cooperation of a witness to obtain the evidence needed in proving the case. Here, the investigator's approach and his/her personal interaction with the witness is usually the determining factor. A private investigator is usually involved in investigations that the SAPS does not deal with. These investigations are wide-ranging, including anything from unethical behaviour in the workplace to civil matters such as matrimonial disputes.

This chapter will attempt to make you aware of certain values that all investigators – both police and private – must subscribe to in order to be successful. You will notice that this chapter is structured to enable all investigators to derive the greatest benefit from it. It will increase your ability to deal with people and will make you a sought-after commodity in the field of forensic investigation.

Please remember that you should not view this chapter in isolation. You should study it in conjunction with the modules in your first year of study. What you learnt in your first year was the basics of investigation, along with an introduction to crimes and transgressions that will be expanded upon this year, as well as in your final year. Each successive body of knowledge thus forms a stepping stone that will lead you closer to your ultimate goal, namely to become a qualified forensic investigator.

I will be dealing with sensitive issues in a forthright manner so that you can understand the difficulties that an investigator is faced with and the importance of overcoming them. The tools to do this are contained in this module and you are urged to pay attention to the content and do the various activities.

2.2 PROFESSIONAL CONDUCT

The word "professional" can be used in different ways. Firstly, it describes the fact that a person does something for his/her livelihood. A professional gambler, for instance, has no other job or source of income; he or she makes a living out of gambling. The same is true of a professional soccer player. However, the term is usually applied to a doctor, a lawyer, an architect or a similarly qualified person who has received specialised training and uses that training to earn a living.

When we refer to professional conduct, however, the word takes on a slightly different meaning. It describes the conduct of a person as being in keeping with his/her unique training and status. The person's status is usually indicated by the way in which he/she is addressed – such as addressing your doctor as "Doctor so-and-so" or an advocate as "Advocate so-and-so". Society has come to expect a special form of behaviour from these persons, who are regarded as being "fit" and "proper". We respect them and expect them always to set an example.

When we refer to "professional conduct", we are referring to honesty and integrity. These are the qualities that all investigators should aspire to. It is this conduct that will ensure that the people you deal with will respect you and want to cooperate with you. Remember that respect is earned. A person with a high rank who behaves in a disgraceful manner will not be respected. The same applies to all investigators – especially a private investigator, who must rely on his/her personality and appearance to impress a witness.

Professionalism is the most important quality when attempting to impress a witness. For instance, would you rather cooperate with a well-spoken, well-dressed person who respects you, or with a person that looks like a vagrant/homeless person? First impressions last. If the first impression that you make on a potential witness is positive, half the battle has been won.

In their book *Practical aspects of interview and interrogation,* Zuwalski and Wicklander (2002) deal extensively with the role that the interviewer/interrogator plays in the ultimate result of an interview or an interrogation. According to these authors, the attitude and strategies or tactics employed by the interviewer/interrogator often cause suspects to deny their part in a transgression or crime.

The authors have identified a number of aspects, all of which relate to professional conduct in one way or another (Zuwalski et al 2002:170) and can affect the outcome of an investigation.

At this point, it is important for you to understand the difference between an interview and an interrogation. An interview is conducted with a cooperative witness, who is aware that all information is given voluntarily. The atmosphere in which this interaction takes place is friendly and relaxed. An interrogation, on the other hand, is a more forceful method, which is designed to place the witness under pressure with the aim of obtaining an admission or a confession regarding some wrongdoing.

ACTIVITY 2.1

1. Make a list of all the items or aspects that you would consider as being important to determine whether an investigator acted either professionally or unprofessionally.
2. List these attributes in order of importance (from most to least important).
3. How would you define the term "professional"?

2.2.1 Personality

I am discussing this issue of personality as a build-up to the discussion of interviewing skills, which will be discussed later in this chapter. I will clearly show the various methods that are used to obtain information. The following discussion involves the personality traits of an investigator to show how these may influence the interview/interrogation process.

It is significant that the subject's perception of an investigator's personality can play a large part in determining whether the investigator will be able to overcome the suspect's fear of the consequences of his/her wrongdoing. Suspects and witnesses are naturally defensive during an interrogation or an interview and investigators who are overbearing and aggressive often cause defensiveness in the subjects, resulting in denial. In contrast, an investigator with a professional personality will help to put a subject at ease because people instinctively trust such persons.

2.2.2 Attitude

While an aggressive and overbearing investigator may increase a subject's defensiveness, an investigator who appears to be weak or unemotional/indifferent may cause a subject to try to

exploit the situation and take control. Your attitude should therefore be positive and professional, not attempting to rush things and pressure a subject into making a confession.

2.2.3 Reputation

You may have heard the saying that a person's reputation precedes him/her. If an investigator has a reputation for being harsh and unsympathetic, he/she is likely to put such fear into the subject that the latter will deny everything. An investigator who has a reputation for fairness, thoroughness and professionalism will have the opposite effect because the subject knows that there will be no trickery or deceit during the encounter.

You should also be aware of the negative effects that transgressions of human rights may have on the investigation – and, of course, your reputation. It has happened in the past that a court of law has found an investigator to be untruthful. Such a finding will have a devastating effect on the future career of the investigator, since the first question a defence lawyer will ask him/her during cross-examination is whether he/she is the same person who was previously found to be an untruthful witness he/she will thus lose all credibility.

2.2.4 Tentativeness and unconvincing behaviour

Verbal and physical behaviour during the session can also directly affect a subject's decision to deny any wrongdoing. Therefore, it is very important that you avoid displaying any sign of being unsure or unprepared. Remember that the subject knows the truth. If they were involved in the transgression, but you are failing to present the facts correctly, the subject will deny everything and leave you to provide the proof. Being unsure demonstrates unprofessionalism.

You must be well prepared and have all the facts at your fingertips. You must also convey conviction in your tone of voice. Don't let the subject get the idea that you are not completely in control of the situation because then you will have already lost the battle, whereas a positive approach by the investigator will lead the subject to believe that he/she has already been caught out.

2.2.5 Perception

As an investigator, your general appearance and the approach you adopt towards the subject during the initial interaction will be decisive in determining what the subject thinks of you. For that reason, you must be completely professional in your approach. You may, of course, decide to adopt a different role and give the idea that you really are not quite sure of what is going on, thereby allowing the subject to tell lies that you can later use against him/her during the confrontational phase. The question, though, is whether this will enhance your reputation as a professional.

ACTIVITY 2.2

1. Make a list of the actions you would take to impress a suspect or uncooperative witness, thus convincing him/her to cooperate with you, without threatening or intimidating them.
2. Make a list of unacceptable behaviour on the part of an investigator during an interrogation session with a suspect.
3. What do you think is the single most important personality trait that an investigator should have?

2.2.6 Wrong rationalisation

This simply means that if you, as an investigator, are able to offer the subject a reason for his/her having committed the offence, it is more likely that the subject will admit or confess and, possibly, want to make a deal with you. For this to happen, you must be in possession of all the evidence and the facts.

You must convince a subject in a professional manner that they have been caught out and yet still allow them an opportunity to give a good reason for having committed the transgression. If you do not concede that there may have been a good reason for their having acted in the way that they did, they will deny everything.

2.3 NEGOTIATION AND ANALYTICAL SKILLS

Negotiation is an art that requires a positive personality trait, namely self-confidence. Persons lacking self-confidence are unlikely to be good at negotiating or establishing a good relationship with a witness or suspect. Zuwalski et al (2002:38) state that a successful interrogator takes on the role of a mediator–negotiator, negotiating from a position of confidence – confidence not only to be able to resolve the problem, but also to be able to understand the suspect and believe in the facts of the case.

2.4 EMOTIONAL INTELLIGENCE

Emotional intelligence, which is abbreviated as EI, is the ability, capacity and skill to identify, assess and manage your own emotions and those of other individuals and of groups. Although this lies within the domain of psychology, it is of great importance to the criminal investigator because it involves dealing with people. All investigators, irrespective of the field they work in and whether they are managers or workers, are in the "people" business. This simply means that they interact with others on a daily basis and therefore need to know how to deal with people in such a way that they get them to cooperate optimally.

2.4.1 Definition of emotional intelligence

There are a number of definitions, but I will give only two here.

The first definition, by S Hein (http://www.eqi.org/eidefs.html) is as follows:

"Emotional Intelligence is the innate potential to feel, use, communicate, recognize, remember, describe, identify, learn from, manage, understand and explain emotions."

The second definition was sourced from Wikipedia (http://en. wikipedia. org/wiki/Emotional_ intelligence**)** and reads as follows:

"Emotional Intelligence (EI) describes the ability, capacity, skill, or in the case of the trait EI model, a self-perceived ability, to identify, to assess and manage the emotions of one's self, of others, and of groups."

To be able to understand EI and what it means to the investigator, it is necessary to mention that there is considerable disagreement among researchers regarding the definition of EI. In addition, researchers are constantly changing their definitions.

2.4.2 Models of emotional intelligence

At present there are three main models of EI, which will be discussed only as far as they are of importance to the investigator. These models are

- the ability EI model
- the mixed model of EI

- the trait EI model

2.4.2.1 The ability model

The ability model views emotions as useful sources of information that help a person to make sense of the social environment. Firstly, it is the ability to detect and decipher emotions in persons' faces, in pictures and in voices. Secondly, it is the ability to use emotions in activities such as thinking and problem-solving. Thirdly, it is the ability to understand the hidden meaning of the language used when a person is emotional, to be sensitive to slight variations in emotions and the ability to recognise and describe how emotions evolve over time.

2.4.2.2 The mixed model

This is important as far as the investigator is concerned because it deals with self-awareness, which is the ability to read a person's emotions and recognise their impact, while using gut feeling to guide decisions. This gut feeling is that inexplicable feeling that you get about something. For instance, while you are busy interviewing a person, you may get a feeling that the person is lying to you; you are able to detect that in the person's reactions/responses to you.

This model also deals with self-management, which involves controlling your emotions and impulses while adapting to changing circumstances. Self-management deals with controlling your temper as well as displaying tact while under provocation or stress. For instance, you may be interviewing a person who responds to you in an aggressive manner, possibly by insulting you racially or threatening you physically.

Social awareness is also very important because it allows you to sense and understand another person's emotions while understanding the social network. For example, you may be interviewing a person who is emotionally upset as a result of being insulted by a person who believes that he or she is better than others. By being aware that there are people who believe that they are more important or of a higher social standing than others, you will be able to interact more successfully with them and also gain their cooperation.

Relation management is, as far as I am concerned, one of the most important abilities that an investigator should have. This is because an investigator deals with so many different people that there are bound to be times when conflict will occur and threaten to destroy a team or prejudice an investigation. Relation management is the ability to inspire, influence and develop others, while simultaneously managing conflict.

2.4.2.3 The trait model

The trait model relates to personality; it involves a person's perception of himself or herself, whether good or bad. For instance, you may be faced with an extremely difficult investigation that presents many challenges; you may not be sure how you will get the evidence that you need; or there may be a difficult witness that you feel uncomfortable interviewing. In such a situation, you may either have full confidence in your ability to deal successfully with this difficult situation/ person, or you may be filled with self-doubt. This feeling, according to researchers, is an inborn personality characteristic called a trait.

2.4.3 Practical application of EI models

Now that I have discussed the various models, let's apply them in practice to see how they affect you, as an investigator. Regardless of whether you are a team member or a supervisor or manager, EI will have a significant impact on you and the way in which you act and react.

It is very important to stress that none of the three models is better than the others. In fact, in a team, you will need investigators with different personalities. As an example, think of the "good cop/bad cop" approach: one investigator plays the real "tough guy", who just wants to arrest the

suspect without even listening to his/her story. He is the so-called bad cop and his approach makes the suspect feel that he/she is not getting any sympathy. The other investigator is the complete opposite: He does not want to arrest the suspect and wants to hear what the suspect has to say in his/her defence. He appears to be very sympathetic to the suspect and the suspect gets the feeling that this investigator wants to protect him/her. Psychologically, the suspect is more likely to cooperate with the investigator that he/she perceives to be the "good cop".

Note that we are not all able to play-act in a convincing manner. There must be a personality characteristic that the supervisor could identify as being valuable in team selection – as is discussed in another module. Therefore, when selecting members of a team, the supervisor will have to identify this particular personality characteristic in an individual. This will be discussed further in another module.

2.4.3.1 The ability model investigator

One thing is very clear: we all have different personalities and we do not react in the same way to challenges. It is therefore very important that the ability model investigator understand the implications of this model, both for himself/herself and the persons that he/she may work with – either as colleagues or as clients. The ability model investigator has a keen sense of other people's emotions and is able to adapt to a particular situation. This investigator has empathy for the feelings of others and might even understand the motive of an offender. This ability could be an advantage, since such investigators could successfully manage emotions in themselves and in others. Researchers believe that these persons are able to harness emotions – even negative ones – and manage them to achieve intended goals (http://eqi.org/eidefs.htm).

- In practice, this would mean that the ability model investigator would be able to get a confession from an offender far more easily by being able to identify potential emotional weaknesses in the suspect, such as body language, tone of voice and language usage, and then adapt his/her approach according to these observations. If you are able to sense another person's vulnerability or weakness, you will most likely have an advantage over the other person.
- What is also important is that if you are an investigator with such EI, you should be aware of it in yourself and be able to manage it to your advantage. The following characteristics are important in an investigator and if you feel that you do not possess them, it may be a good idea to develop them consciously.

Characteristics to be aware of:

- self-understanding
- your personality profile
- your weaknesses, strengths and EQ gaps

Characteristics to improve or develop:

- interpersonal skills
- listening and communication skills
- feedback skills
- assertiveness skills
- focusing on the good in yourself and others
- emotional resilience and hardiness
- ability to identify emotions and feelings and then release them
- an understanding of your personal mission and passion

2.4.3.2 The mixed model investigator

The investigator with this EI could be referred to as an "all-rounder". With this EI, such an investigator is capable of being used in most investigations because of having such an adaptable personality. This investigator has a sixth sense that tells him/her when somebody is lying. Of course, there are also external signs that indicate when a person is lying. These include

- dry lips
- perspiration
- clammy hands
- shortness of breath
- change in skin tone

Source: (Swanson, Chamelin & Territo 1977:153)

Let's now examine why this investigator is so well suited to investigative work. Firstly, he/she has an even temper, which means that emotions do not play a role when conducting an interview or interrogation. Some investigators have a tendency to be short-tempered or aggressive, which immediately antagonises the subject and could jeopardise the investigation. As you will see in the discussions below, a successful investigator has many qualities, the most important of which is people skills.

Any assault on an accused or a suspect is not only highly illegal, but also unprofessional and brings the whole investigation function into disrepute. It will also destroy the case.

The EI investigator will always ensure that, as far as possible, the ethnic, religious or other sensitive issues relating to the subject are taken into consideration during an interview. There are many aspects that could cause the subject to take offence, which the investigator might not even be aware of. One example is eye contact. In some societies, making eye contact is regarded as a sign of aggression. In other societies – for instance certain Arabic countries – displaying the soles of one's feet while sitting is regarded as a sign of contempt. So, while you cannot be expected to be aware of all the pitfalls associated with dealing with people from diverse cultural backgrounds, you could try to ask a person from that cultural background to assist or advise you on what to avoid. It all boils down to respect. If you respect the other party – irrespective of who they are or what they may have done – you will earn their respect, which will make your job much easier.

2.4.3.3 The trait model investigator

A person with an offensive personality can do irreparable damage to an investigation, since he/she will continually antagonise others. This individual may suffer from an inferiority complex and may try to compensate for this by being bombastic or insulting towards others. They may even be bullies, who abuse their power over others. This often happens when an unqualified person is placed in a position of leadership; they attempt to compensate for their shortcomings or inferiority complex by being aggressive and insulting.

The importance of selecting the correct person for the job cannot be overemphasised. This is especially true when selecting a team to investigate a complex case. Team members must be compatible, otherwise conflicting personality traits will hamper the functioning of the team and undermine the investigation.

A person with a strong will and a clear sense of direction will benefit the team, especially when it comes to boosting their morale. But if such a person, as an investigator, is not properly managed, he/she may easily take over, which could lead to serious disciplinary issues in the team (e.g. a strong-willed individual may resent yielding to any higher authority because he/she has feelings of superiority).

The investigating manager who is faced with this situation should ensure that the rest of the team members that will be working with such a person are properly selected, otherwise what is called "clan-forming" will take place. This refers to team members' aligning themselves with two or even more supervisors and then competing against the others.

If there is such a danger, it is advisable to seek professional assistance from a psychologist. This person will be able to conduct personality tests and advise you on the selection of a suitable team. You may feel that this is not necessary, but should you fail to attend to this very important aspect

and your team selection proves to be wrong, there will be such internal conflict between the team members that your investigation will suffer and may even be ruined.

One last thought on this issue that may be of interest is the influence that alcohol has on team unity. On the face of it, team members may appear to be compatible, but as soon as they start to consume alcohol – for instance when the team members are relaxing together over some drinks after a long day or a stressful week – small cracks that have been latent might suddenly appear and members might start to argue. These arguments may be insignificant at first, but could later become heated and aggressive. Before you know it, members start taking sides and you have a problem that you must deal with swiftly and decisively – even if it means dropping certain persons from the team.

Nevertheless, it is very important that team members relax – especially where internal investigations are concerned, since these involve extremely sensitive issues. Staff members may not wish to cooperate as they would for an external investigation, for fear of being regarded as a sell-out or a traitor by the others. Therefore, they tend to regard internal investigators as the enemy and avoid contact with them.

As a manager, you will quickly come to realise how difficult it is to raise the morale of members of a team who have been shunned by their former colleagues. Conducting an internal investigation is an extremely stressful activity, which also affects the member's family. You must therefore be aware of these challenges and prepare your team for this eventuality. Ensure that you are able to obtain professional assistance when the first signs of stress start to show, which usually manifest in aggression and intolerance.

ACTIVITY 2.3

Assume that you are leading a team that is mixed in terms of race and gender. You have been tasked to investigate a syndicate dealing in drugs and prostitution. You need an investigator who is able to infiltrate the syndicate and become accepted by them. Your preference for the job is a member who has recently been promoted and who is highly recommended. This person has all the necessary qualities for the job and, being a homosexual himself, he is able to identify with various groupings in both the gay and straight communities.

However, there is resentment toward this person and members of the same gender refuse to become involved. Your problem is that one of the greatest critics of this member is also the best at dealing with hostile and aggressive persons. The challenge is to find a way of getting these two members to cooperate, since you have decided to establish a small team of no more than (four) members to conduct the investigation.

After having considered the different EI models, answer the following questions:

1. Which EI model investigators would you select to become part of the team?
2. Would you consider including members of the opposite sex in the team?
3. If you had a choice – and those persons were available – which EI model investigators would you select to perform the various tasks, such as providing back-up for the team, subtly obtaining information, winning the trust of syndicate members and, if necessary, taking drugs?

2.5 ETHICAL CONDUCT

"Ethics can be defined as the study of what is right and good in conduct. It is the general theory of conduct and considers the actions of human beings with reference to their rightness or wrongness, their tendency to do good or evil" (Tshaka 2010).

The concept of ethics is often confused with the concept of morality. The difference between the two lies in the fact that "ethics" is derived from the Greek word *ethos*, which means "character" and is related to custom or habit. On the other hand, morality, or *mores*, refers to norms and values that are designed to give form to a particular community or society; this concept refers to a behaviour pattern. In this sense, we speak of a moral act or a moral person, but an ethical system or code.

"Ethics is a practical thing. It is a way of conduct. It is only practical when it is being practiced" (Tshaka 2010).

Ethics should not be confused with morality. Morality is a behavioural issue, while ethics is something derived from society. This means that if a community regards certain behaviour as being ethical according to its standards, that particular behaviour may not necessarily be legal (Tshaka 2010).

Iannone (1980:80) refers to "leadership ethics" and is of the opinion that "the position of true leadership places upon the leader a moral obligation to adhere strictly to high standards of honor and integrity he expects from his subordinates and which they and his superiors have the right to expect of him." This refers to a moral code, which must be beyond reproach. Not only must the leader avoid all evil, but his conduct is evaluated in terms of what it is, what he/she thinks it is and what it appears to be to others. This is applicable not only to leaders, but to all investigators. Integrity is non-negotiable.

Prof Tshaka (2010) is of the opinion that there is a certain bond that holds society together. If this bond is attacked, society becomes fragmented. The question, then, is: Why do people obey the law? Do they do so as a result of ethical persuasion or because of fear? Investigators should keep these questions in mind. The reasoning seems to be that if the detection rate of crime were increased, there would be a corresponding increase in the chances of arresting criminals; this, in turn, would encourage people to be ethical because of the strong chance that criminals would be detected and arrested.

Given the lack of ethics in society today, it is relevant to consider where ethics originate: is in the home, at school, at university, in the workplace or in society as a whole? And how do we restore ethics to a society that has ceased to be ethical?

These questions are very important to investigators because if an investigation requires the assistance of a society that is hostile to the idea of investigation, there is very little chance of success. For example, consider an internal investigation that is being conducted within a section (unit) of the police service. Because there is such strong social and ethical cohesion among the members of that unit, the investigator would find it very difficult, if not impossible, to break through that barrier and get members to disclose incriminating information about one another.

2.5.1 Code of Conduct for the Public Service

Below I will quote from the Code of Conduct for the Public Service to illustrate the importance of such a code in the workplace. Not only is it a guide for employees in how they should conduct themselves in their relationship with their employer, but it is also a good way to determine a person's frame of mind when you are conducting an investigation into an alleged contravention.

All employees are expected to know the code of conduct that their organisation subscribes to. If you, as an investigator, are able to prove the existence of such a code and the fact that the employee was aware of it, the sanction imposed on a transgressor could be severe.

Although the Code of Conduct for the Public Service was designed with South African public servants in mind, it is worthwhile quoting this code in its entirety because of its universal applicability. This code was developed in 1997 and was promoted through workshops with officials at various levels of the public service.

In the introduction to the Explanatory Manual on the Code of Conduct for the Public Service, officials are urged to think and behave ethically. It quotes section 195(1)(a) of the Constitution, which "requires that a high standard of professional ethics must be promoted and maintained" in public administration generally. It goes on to state quite categorically that "the primary purpose of the Code is a positive one, to promote exemplary conduct". It states that an employee will be guilty of misconduct if he or she fails to comply with any provision of the code.

Code of Conduct for the Public Service

C. CODE OF CONDUCT

C.1 RELATIONSHIP WITH THE LEGISLATURE AND THE EXECUTIVE

An employee –

C.1.1 is faithful to the Republic and honours the Constitution and abides thereby in the execution of his or her daily tasks;

C.1.2 puts the public interest first in the execution of his or her duties;

C.1.3 loyally executes the policies of the Government of the day in the performance of his or her official duties as contained in all statutory and other prescripts:

C.1.4 strives to be familiar with and abides by all statutory and other instructions applicable to his or her conduct and duties; and

C.1.5 co-operates with public institutions established under legislation and the Constitution in promoting the public interest.

C.2 RELATIONSHIP WITH THE PUBLIC

An employee –

C.2.1 promotes the unity and well-being of the South African nation in performing his or her official duties;

C.2.2 will serve the public in an unbiased and impartial manner in order to create confidence in the Public Service:

C.2.3 is polite, helpful and reasonably accessible in his or her dealings with the public, at all times treating members of the public as customers who are entitled to receive high standards of service;

C.2.4 has regard for the circumstances and concerns of the public in performing his or her official duties and in the making of decisions affecting them;

C.2.5 is committed through timely service to the development and upliftment of all South Africans;

C.2.6 does not unfairly discriminate against any member of the public on account of race, gender, ethnic or social origin, colour, sexual orientation, age, disability, religion, political persuasion, conscience, belief, culture or language;

C.2.7 does not abuse his or her position in the Public Service to promote or prejudice the interest of any political party or interest group;

C.2.8 respects and protects every person's dignity and his or her rights as contained in the Constitution; and

C.2.9 recognizes the public's right of access to information, excluding information that is specifically protected by law.

C.3 RELATIONSHIP AMONG EMPLOYEES

An employee –

C.3.1 cooperates fully with other employees to advance the public interest;

C.3.2 executes all reasonable instructions by persons officially assigned to give them, provided these are not contrary to the provisions of the Constitution and/or any other law;

C.3.3 refrains from favouring relatives and friendsin work-related activities and never abuses his or her authority or influences another employee, nor is influenced to abuse his or her authority;

C.3.4 uses the appropriate channels to air his or her grievances or to direct representations:

C.3.5 is committed to the optimal development, motivation and utilization of his or her private staff and the promotion of sound labour and international relations;

C.3.6 deals fairly, professionally and equitably with other employees, irrespective of race, gender; ethnic or social origin, colour, sexual orientation, age, disability, religion, political persuasion, conscience, belief, culture or language; and

C.3.7 refrains from any party political activities in the workplace.

C.4 PERFORMANCE OF DUTIES

An employee –

C.4.1 strives to achieve the objectives of his or her institution cost-effectively and in the public's interest;

C.4.2 is creative in thought and in the execution of his or her duties, seeks innovative ways to solve problems and enhances the effectiveness and efficiency within the context of the law;

C.4.3 is punctual in the execution of his or her duties;

C.4.4. executes his or her duties in a professional and competent manner;

C.4.5 does not engage in any transaction or action that is in conflict with or infringes on the execution of his or her official duties;

C.4.6 will recuse himself or herself from any official action or decision-,king process which may result in improper personal gain, and this should be properly declared by the employee;

C.4.7 accepts the responsibility to avail himself or herself of ongoing training and self-development throughout his or her career;

C.4.8 is honest and accountable in dealing with public funds and uses the Public service's property and other resources effectively, efficiently and only for authorized official purposes;

C.4.9 promotes sound, efficient, effective, transparent and accountable administration;

C.4.10 in the course of his or her official duties, shall report to the appropriate authorities, fraud, corruption, nepotism, maladministration and any other act which constitutes an offence, or which is prejudicial to the public interest;

C.4.11 gives honest and impartial advice, based on all available relevant information to higher authority when asked for assistance of this kind; and

C.4.12 honours the confidentiality of matters, documents and discussions, classified or implied as being confidential or secret.

C.5. PERSONAL CONDUCT AND PRIVATE INTERESTS

An Employee –

C.5.1 during official duties dresses and behaves in a manner that enhances the reputation of the Public Service;

C.5.2 acts responsibly as far as the use of alcoholic beverages and any other substance with an intoxicating effect is concerned;

C.5.3 an employee shall not, without prior written approval of the Head of Department obtain or accept any gifts, benefits or item of monetary value (a description and the value and source of gift with a value in excess of R350) from any person for himself or herself during the performance of duties as these may be construed as bribes;

C.5.4 does not use or disclose any official information for personal gain or the gain of others; and

C.5.5 does not, without approval, undertake remunerative work outside his or her official duties or use office equipment for such work" (Public Service Commission 2002:58).

ACTIVITY 2.4

Draw up a code of conduct that you feel would be applicable to your particular sphere of investigation.

2.6 ABSTRACT AND LATERAL THINKING

Before you proceed with this section, I would like you to review the five-questions rule that was described in the module for FOR1501A, which is very relevant to this discussion.

Every investigator should consider his or her options before embarking on an investigation. No investigator would ever start an investigation if he or she did not intend completing it successfully.

2.6.1 Abstract thinking

The basis of abstract thinking is to be able to see what lies behind what is immediately apparent. In other words, things are not always what they seem, and abstract thinking is the ability to see the real issue (http://www.wisegeek.com/what-is-abstract-thinking.htm).

Abstract thinking helps to solve problems in more creative ways by encouraging people to think "outside of the box". This implies that people have a natural tendency to be limited by borders. If, for example, a person is given a drawing of a circle or a square or a rectangle and asked to use it in a sketch, some will sketch something within the borders of the drawing, while others will go outside the borders of the drawing and use it as part of a larger sketch. This ability to think beyond borders is what is referred to as abstract thinking. It is also known as creative thinking.

Based on this perspective, the first of the five questions that an investigator should ask at the outset of an investigation becomes relevant, namely: What have I got?

- What have I got?

The essence of abstract thinking is to analyse the situation by firstly determining what you are faced with. In so many cases, the real issue may be hidden by a number of side-issues that tend to distract you from the core issue. For instance, you may be faced with what appears to be a suicide: all the indications are there, but in actual fact it is a murder that has been made to look like a suicide. If you are not able to think abstractly, you may fail to see the real issues and will conduct the investigation in a totally different way from how you would have if it had been a murder. Consider all possibilities and ask yourself the question: What if…? This involves looking at other possibilities.

ACTIVITY 2.5

1. Do you agree that it is important to know what it is that you are investigating before you even start?
2. If so, why do you say so?

3. If not, why not?

2.6.2 Lateral thinking

The term "lateral thinking" was coined by Edward de Bono in his book *New think: the use of lateral thinking,* which was published in 1967 (http://en.wikipedia.org/wiki/Lateral_thinking). It refers to problem-solving through an indirect and creative approach.

Lateral thinking goes hand in hand with abstract thinking. Once you have seen the real problem (What have I got?), the next step is to find the answer. This is where the second of the five-questions rule comes in, namely: What do I need?

- What do I need?

Here lateral thinking is important because it is the practical approach to solving the problem. You evaluate the situation, you know what has happened and now you need to be creative in finding the answer. The remaining three questions of the five-questions rule are also involved in the lateral thinking process, namely: Where do I get it? How do I get it? and What do I do with it? As you can see, the answers to these questions are all part of the solution to the problem. In many instances, you may be faced with a hostile witness or you may be unable to obtain vital evidence. You must then be creative in the problem-solving process – which is all part of lateral thinking.

2.7 VERBAL AND WRITTEN COMMUNICATION

Communication is an art and it is an essential part of most occupations. For example, a person who is unable to communicate effectively will not be able to promote his or her business or do a proper presentation on the findings of a job that he/she has done. Communication is also vital to the success of any investigation.

2.7.1 Verbal communication

The most obvious form of verbal communication is the daily discussions that you have with other people. These are so numerous that I will refer to only a few that are important for this discussion.

- In court

Investigators may testify in various courts of law, from magistrates' courts to the High Court in both civil and criminal matters, as well as in disciplinary and administrative hearings. These hearings require that the witnesses give verbal testimony regarding a wide range of subjects so that the presiding officer is able to understand what transpired and make a decision or a finding.

A witness is assumed to be well prepared and aware of what is required of him/her before he/she enters any court or administrative hearing. However, this is often not the case, with the result that the person's testimony is discredited and the evidence not accepted.

- Verbal presentations

Anxiety is one of the major obstacles to a good presentation. You may lack confidence or fear that you will say something that makes you appear foolish. But it is important to realise that your fear is basically undermining you, and the only way you can overcome this is by developing a positive attitude about the presentation. English et al (2006:216) provide the following table on essential skills to ensure effective presentations:

TABLE 2.1

Anxiety	**Skill**
1. Symptoms such as a feeling of overall anxiety and a general lack of confidence; fear of appearing foolish; mentally undermining you.	Develop a positive attitude about the presentations. Our attitudes dictate our behaviour. We can change negative perceptions/thoughts into positive ones and consequently we will appear confident.
2. Physical manifestations of nervousness such as shaking knees, butterflies in the stomach and a dry mouth	Relax areas of tension and breathe deeply. Use correct body language/nonverbal cues that include handling and using correct visual aids.
3. Fear of forgetting the content.	Use note cards with key phrases on them or informative visual aids to jog your memory. Do not write out full sentences and then read or try to memorise them.
4. Fear of being ineffective or alienating The audience; fear that the audience might be bored or not understand what you are saying.	Analyse your audience and their needs carefully in order to plan and select your information to meet those needs. Establish rapport with your audience.

Source: English et al 2006:216

ACTIVITY 2.6

1. Make a list of some additional issues that you feel may contribute to feelings of anxiety that could hamper your ability to give verbal evidence.
2. Describe any feelings of anxiety that you may have experienced in the past.
3. What did you do to overcome these feelings and were you successful in doing so?
4. What was the result?

Many verbal presentations are accompanied by computer-aided PowerPoint presentations. In this regard, English et al (2006:274) suggest the following general principles:

- First gather the text and then the graphics.
- Choose a title for your presentation.
- Summarise your points with phrases rather than with whole sentences because you oral presentation will include the detail.
- Use no more than five or six lines per slide and no more than six words on a line.
- Keep charts and graphs simple, without too many elements such as lines and colours.
- Show trends rather than detailed data.
- Ensure that your visuals can be understood in 15 seconds after first viewing. They must reinforce what you are saying.
- Use bright and contrasting colours to help your audience read the text easily.
- Make sure that the lines are thick enough for easy visibility.

2.7.2 Written communication

The structure and the format of written reports are dealt with later in this module, where I will discuss the content of the written communication and the importance of getting the correct message across.

The importance of written communication cannot be over emphasised. You must always remember that the person reading your report or statement has no knowledge of the matter and must make a decision based on what you have written and recommended.

2.8 INTERVIEWING SKILLS

Interviewing can take one of a number of different forms, depending on the type of person that is being dealt with. The different types of persons are described below:

- **Complainants and victims**. These are persons directly involved in the crime, who have suffered some kind of loss or injury. In some cases, they may not be directly involved, but are complainants as a result of their employment position. For example, they may be a financial officer or another responsible person laying a charge as a result of some criminal offence that has been committed in the workplace. Normally, however, they are the persons who are able to give first-hand evidence regarding an offence or a transgression because they are victims.
- **Witnesses – both reluctant and hostile**. Witnesses are sometimes reluctant to come forward and present themselves, partly because they feel guilty about "informing" on somebody. This could be because they know the suspect and don't believe that he/she is guilty or involved in the transgression, or because the suspect is a friend or a family member. They may fear being shunned by society or being cast out by family members (Zuwalski et al 2002:189). In contrast, hostile witnesses evade being interviewed and, when confronted, deny any knowledge of the matter or refuse to be interviewed. When this happens, it is advisable to make use of legal remedies, if possible; if not, try to avoid using the person as a witness. Remember that a witness may be declared a hostile witness by the prosecutor if there is any indication that the witness has changed or deviated from his or her original statement. In such a case, the prosecutor may cross-examine his or her own witness.
- **Suspects**. They are also witnesses. Not all suspects will become accused; therefore, their testimony may become relevant, should they decide to become witnesses for the state. In such cases, you are advised to discuss the matter with the prosecutor.
- **Accused persons**. They are witnesses for themselves. The only interaction that you will have with such a person is in the initial interview and when recording a formal exculpatory statement. You must always keep an accused's constitutional rights in mind. Remember that the accused has the right to legal representation and any attempt on your part to convince him or her to waive that right is unconstitutional and, possibly, illegal. When dealing with an accused who indicates that they will make a statement only after consulting with their legal representative, you must respect that decision and not pressure the accused any further by making promises or threats.

Even if you are a private or corporate investigator, you have to be careful in your dealings with a suspect or an accused person. You have to be aware of the fact that a person cannot be forced to make any admission or a confession; any attempt by you to do so will be regarded as extraction and the resulting evidence will be declared inadmissible.

ACTIVITY 2.7

In your own words, describe what you understand "extraction" to mean and explain why you consider it unacceptable.

2.8.1 Interviewing

Interviews start with known witnesses. This means that those persons whose names are known at the start of an investigation are the first persons to be interviewed. During the interview, further information becomes available and the witness may reveal the names of other persons involved in one way or another.

The purpose of an interview is to gather and verify relevant information (Van Rooyen 2004:194). For that reason, your questions must be clear, specific and unbiased. An interview is exploratory in nature, meaning that it is conducted to gather information. The interview is therefore a discussion to find out what the person knows and whether it may be of importance for the investigation. A question-and-answer session is non-confrontational, as it is the prelude to the investigation itself. It is only when most of the facts become apparent that a decision is made about who the possible suspects are.

Interviews usually follow a certain routine, with the interviewer setting the tone and giving background on the reason for the interview. However, it is important to be careful not attempt to influence the witness by making your own feelings known, since this could cause the witness to say what he or she thinks you want to hear. This is especially true when interviewing youngsters.

The so-called cognitive interview technique, as a method to get the best information from a witness or a victim, is preferred by many investigators. This technique involves the following (Zuwalski et al 2002:229):

- Establish rapport. The interviewer starts the process by establishing rapport with the witness.
- Reconstruct the circumstances of the event. The witness is asked to reconstruct the events by giving some background information. In this way the witness is "warmed up" and is able to re-construct the event. The witness is asked to think about aspects such as the weather, lighting or the general appearance of the environment in which the incident took place.
- Report everything. The witness should report everything that took place, without being selective or omitting anything, no matter how trivial. The witness is not the person to decide whether anything is relevant or not. Using open-ended questions encourages a witness to speak. Interruptions should be kept to a minimum, as this may distract the witness and break their train of thought. Be sure to keep notes of what the witness says so that you can return to certain issues that are either unclear or need further explanation.
- Recall the events in a different order by asking the witness to start from either the middle or the end and go back to the beginning. For instance, use a particular incident that the witness reported and ask him or her to go back and tell you about it. Here, in particular, open-ended questions can be of great value.
- Change perspectives by asking the witness what he or she would have done had he or she been in the same position. Also ask the witness about possibilities that could have had an influence on his or her perception of what happened.

According to Zuwalski (2002:229), the basic value of the cognitive interviewing technique is that it reconstructs the circumstances in a number of different ways in the witness's mind.

2.8.2 Questioning

By the time the process reaches the stage where you are reasonably sure who the suspects are and who the witnesses are, your quest for information has reached a different level. You have finished the interviews and discussions and you are in a position to take a more focused approach to the investigation; by now you have a good idea of which witnesses will be able to provide more specific information on the subject. Van Rooyen has developed a table that sets out the differences between interviews and interrogations.

TABLE 2.2

Differences between interviewing and interrogation

INTERVIEWING	INTERROGATION
PURPOSE Obtain information.	Obtain a confession.
ENVIRONMENT Comfortable, relaxed, congenial; interruptions, although undesirable, can be tolerated.	Strictly controlled. No distractions (pictures, posters or paintings) and no interruptions whatsoever.
SEATING Fairly comfortable; armrests; table nearby to write on.	Hard to semi-hard chair and about 50 mm lower than the interrogator's chair. No armrests, which would enable the subject to prop himself/herself up and delay or prevent body structure collapse.
CONTROL The subject controls the process, while the interviewer directs it.	The interrogator dominates, controls and directs the process.
COMMUNICATION 95%:5% – Subject:Interviewer. Subject communicates as much as possible.	5%:95% – Subject:Interrogator. Interrogator communicates the most. Subject is brought to the point of confession and confirmation.
PREPARATION Knowledge of the crime and the subject's link to it.	In-depth knowledge of the crime and the subject's link to it. Knowledge of the subject; his/her work; home background; financial status; relationships with family, friends and colleagues; and most likely reason for committing the crime.
BREAKS Frequent breaks for refreshments. Smoke breaks are allowed.	No breaks allowed for the first two hours.

Source: Adapted from Van Rooyen 2004

As can be seen from the table above, there is a difference between the attitude of the interviewer and the interrogator. The interview is far more relaxed and friendly than the interrogation.

During the interview, the interviewer encourages the subject to talk by asking open-ended questions that are designed to get him or her to expand on previous answers. The open-ended question technique is referred to as the TED technique, which stands for tell, explain and describe. When applying this technique, if you start a question with any of these words, you are actually inviting an answer.

Open-ended questions are the opposite of closed-ended questions, where the subject is asked a question that may be answered with a simple "yes" or "no" or something similar. The difference between an interview and an interrogation is that an interview is a non-accusatory fact-finding exercise between the interviewer and the subject.

2.8.3 Interrogation

Interrogation is formal and systematic questioning to learn the facts. Please refer to table 2.2 above to see the distinction between interrogation and interviewing. The purpose of interrogating is to obtain an admission or a confession from the subject.

Zulawski et al (2002:18) state that no matter how an investigator chooses to interrogate a suspect, there will be four distinct parts to the confrontation:

- *Reducing resistance.* The interrogator chooses some method to reduce the suspect's resistance to a confession. Take care that these methods are not in violation of the suspect's constitutional rights or those determined by the Judges' Rules. This could be done with a systematic presentation of evidence, the use of emotional appeal or the professional approach of the interrogator.
- *Obtaining an admission.* Obtaining an admission is not the same as obtaining a confession and these should not be confused. It involves getting the person to admit involvement in or knowledge of the offence.
- *Development of the admission.* Once the admission has been obtained, the interrogator can expand on the inquiry by asking more searching questions to determine whether the suspect was involved in other crimes. This may also result in the suspect's making a formal confession.
- *Professional close.* The interrogator then closes the matter by obtaining a statement from the suspect. This is usually an exculpatory statement, which differs from a confession. In this regard, the suspect's constitutional rights are clearly set out and respected.

An interrogator should never allow the subject to take control of the process. This could easily happen if the subject has a friendly attitude and asks the interrogator questions, which the interrogator would feel uncomfortable ignoring for fear of being rude. Remember that the subject is not your friend, but nor is he/she your enemy, so you should treat him with dignity and respect.

ACTIVITY 2.8

Can you think of ways in which a subject could take over the conversation? How would you regain control of the situation?

2.9 SUMMARY AND CONCLUSION

It is vitally important that investigators know not only the law and the rules surrounding an investigation, but also how to report on their findings in such a way that the recipient is able to make an informed decision. The conduct and professionalism of investigators are extremely important. If the interviews, questioning or interrogation are not conducted properly, the case under investigation may not secure a conviction. The courts and other quasi-judicial forums depend on evidence brought before them to draw certain conclusions. Obtaining the information on which a report is based must be a legal and transparent process. This involves not only questioning and interrogation, but also the use of recording apparatus such as recorders and other devices that are able to capture and store images and voice recordings.

PART 2

Crimes and transgressions

Contents

Chapter 3

Possible indicators of crimes and transgressions

Contents

3.1 INTRODUCTION

In the corporate environment, a fraudulent transaction or suspicious payment could be discovered by an internal auditor during a routine audit or by an auditor conducting a due-diligence investigation of a company on behalf of a prospective buyer; this could result in a report or an allegation being made. Shareholders, disgruntled employees and even scorned lovers are just some examples of the sources of information on suspected criminal activity, which may be necessary to compile a report.

Authorities the world over are taking measures to combat and detect crime. These measures include legislation that deals with money laundering, terrorist financing, corruption and drug

trafficking, to name but a few. Governments are signatories to treaties to ensure that member states implement measures that enforce compliance with resolutions agreed upon. Punitive measures might be imposed on non-member states or non-compliant member states. Statutory measures might have to be implemented by member states to give effect to these treaties, which may include statutory obligations imposed on certain individuals to report crime. Further statutory obligations may require that reports be investigated.

Corporate governance requirements and obligations require that fraud and ethical risks be managed by corporate entities and their subsidiaries. Du Plessis, Mc Cornvill and Bagaric (2005:2) state the following:

> Corporate governance describes the framework of rules, relationships, systems and processes within and by which authority is exercised and controlled in corporations. Understood in this way, the expression 'corporate governance' embraces not only the models or systems themselves but also the practices by which exercise and control of authority is affected.

In South Africa, corporate governance was institutionalised by the publication of the King Report on Corporate Governance in November 1994. Its purpose is to promote the highest standards of corporate governance in South Africa. The Public Finance Management Act 1 of 1999 regulates financial management in both the national and provincial government. Its object is to secure transparency, accountability and sound management of revenue, expenditure, assets and liabilities of the departments, institutions and public entities to which it applies.

In this section we will be looking at the detection of crimes or transgressions, the different forms it may take and some of the responses to it. We will also look at statutory crime-reporting obligations in the South African context and the responses to it imposed by law, such as the protection of whistle-blowers and the duty to report certain illicit conduct or a suspicion thereof.

3.2 INVESTIGATION PROCESS

Every investigator should be conscious that an investigation has a life cycle: there is a beginning, middle and an end (Silverstone & Sheetz 2004:121). An investigation can be regarded as a process. The investigation process can be divided into six stages or steps. These stages or steps may overlap and, therefore, some authors may either increase or decrease the number of steps.

This chapter deals with the first stage or step in the investigation of a crime or transgression, namely those events, observations, indicators, reports or activities that lead a reasonably prudent person to believe that a crime or transgression has been committed, may have been committed or is going to be committed. The typical response to such an assertion would be to report the matter to – or to lodge a complaint with – the appropriate investigation authority or person.

Innes (2003:176) views the investigation process as follows: "Crime investigations are composed of a number of discrete yet linked investigation actions, which are directed towards the production of knowledge about how and why a crime or transgression was committed."

According to the combined views of Innes (2003:176), Swanson et al (2003) and Silverstone and Sheetz (2004:120), the investigation process shows how an investigator undertakes a series of sequential actions, from the time the crime or transgression is reported until the case is concluded in court. The main events of this process are as follows:

- crime or transgression reported or discovered
- preliminary investigation
- follow-up investigation
- suspect development and apprehension
- case construction
- hearing or trial

For the purpose of this chapter, only the first event, namely the reporting or discovery, will be elaborated upon.

Reporting a crime or transgression, or receiving a report, normally occurs in the initial stage of an investigation. Reports can take many forms and may be made verbally or in writing. The report can also be made through different mediums, such as telephonically or electronically. Reports may be made by or received from a variety of individuals, who do so because of a moral sense of obligation, a statutory duty imposed on them or a fiduciary duty.

The reports may be received by the investigator, investigation authority or law enforcement agency, either from the person detecting the crime or transgression or from the person to whom such a report was made. Whatever the case may be, there will be a source or an indicator of a crime or transgression. In the next paragraphs we will look at the possible sources, indicators and reporting mediums of crimes and transgressions.

3.3 DETECTION OR DISCOVERY

Everything should be done by the authorities and employers to reduce the risk of crimes and transgressions. Unfortunately, it is a fact of life that crimes and transgressions will occur, no matter how hard the authorities and employers work to prevent them. That is why all organisations should have processes in place to assist in the detection and prevention of crimes and transgressions.

In this chapter we deal with the responsibility for detecting crimes and transgressions, the roles played by the different parties involved, as well as the means of detection. The means of detection include

- red flags
- whistle-blowers
  - hotlines
  - suspicious activity reporting
  - protected disclosures
- statutory reporting obligations and duties
- audit procedures

3.3.1 Red flags

Since organisations cannot prevent all fraud, the auditors, accountants, security personnel and ethics divisions have to be equipped with some detection techniques to be able to deal with the act of fraud, the conversion of the benefit for use by the fraudster and the act of covering up the crime. Catching people in the act of committing fraud is difficult and unusual. The act of conversion is equally difficult to observe, since it will typically occur away from the organisation's premises (Robertson 1997:200).

Many frauds are detected by noticing or observing telltale signs or signals that fraud may be occurring, or has been perpetrated, and then following the trail of missing or falsified documents that are part of the cover-up (Robertson 1997:200). Sometimes the behaviour of an individual, the appearance of a document or transaction or even unusual system activity raises a question mark in the mind of a friend, work colleague or third party. If the person is astute, the incident may be followed up, sometimes to expose a potentially serious problem (Iyer & Samociuk 2006:76).

TABLE 3.1

Examples of 'red flags'	**Reactive**	**Proactive**
Behavioural	Noticing that some managers are reluctant to give proper explanations as to why certain budgetary decisions are made	Performing background checks to identify unsanctioned involvement in external companies
Transactional	Treasury and payment personnel question payments of suspicious invoices to tax havens, such as the BVI and Cayman Isles	Looking for potentially collusive sales transactions where there are unusual patterns of low prices and credit notes
System	Repeated systems failure and audit log switched off	Monitoring and analysis of unsuccessful access attempts to sensitive systems and data
Corporate	Noticing that a sequence of acquisitions and joint ventures failed	Annual personal financial statement and conflict of interest statement completed by executive and verified by external party

Source: Iyer & Samociuk 2006:77

The table above illustrates some examples of both reactive and proactive red flags, which are listed as "behavioral, transactional, system and corporate" (Iyer & Samociuk 2006:77).

By being aware of the indicators of potential problems, or red flags, an organisation can make huge advances in reducing the instances of fraud and corruption (Iyer & Samociuk 2006:77). Iyer and Samociuk (2006:77) assert that a red flag is only an indicator of a potential problem, which may include fraud, corruption or some other malpractice. They have chosen to categorise red flags as being behavioural, transactional, system or corporate. Ultimately, all four categories can be indicative of abnormal behaviour.

Accordingly, each category can be further classified into those that can be noticed by the trained eye, called "reactive red flags", or those that need the help of a detection or corporate health check process; the latter are called "proactive red flags" (Iyer & Samociuk 2006:77).

Red flags can be recognised through observation, either by accident or by a trained person, during the course of business activities.

3.3.1.1 Recognising behavioural red flags

Red flags in behaviour and lifestyle are an indication that an employee may have a problem. Behavioural red flags can be objective in the sense that they can be measured or monitored, or they can be subjective in the sense that they rely on personal knowledge of the individual.

Objective behavioural red flags can include

- signs of excessive wealth or spending
- long absences from work and poor timekeeping
- failure to take vacation or sick leave
- changes in work patterns; working long hours after normal working hours
- repeated overriding of normal controls and procedures

Subjective behavioural red flags can include

- abnormal social behaviour
- problems with gambling or drug or alcohol abuse

- excessive mood swings, aggression, marked changes in behaviour
- resistance to audit and questions, such as confrontational, arrogant and aggressive approach to avoid answering questions and deflect attention
- misleading and ambiguous explanations to questions

Source: Iyer & Samociuk 2006:77

3.3.1.2 Recognising transactional red flags

The vast number of processed transactions resulting from modern work processes can present opportunities for effective transaction monitoring because of the declining cost of storing electronic data. Depending on the nature of the business undertaken by the organisation, red flags can include the following:

- unusual supplier relationships
- intermediaries, business partners, etc, which are actually front companies
- non-transparent counterparties, where indications of criminal association exist
- payment for services and goods of which the detail is vague
- preferential supplier treatment and/or a lack of transparent and competitive tendering processes
- preferential customer treatment
- receipt of potentially ill-gotten gains
- ghost employee salaries or benefits
- private expenses processed through expense claims

Source: Iyer & Samociuk 2006:77

Transactional red flags indicative of fraud and corruption include the following:

- kickbacks paid to management on the acquisition or disposal of subsidiaries, using a tax haven as a vehicle
- company-controlled slush funds and the payment of bribes to and from offshore companies
- secret bonuses to top managers and executives, which are most commonly paid into accounts in tax havens
- money ostensibly for bribes paid into the executive account and employee-controlled accounts
- hiding a conflicting ownership interest in a supplier, customer and business partner, using a cascade of offshore companies to disguise the ownership

Source: Iyer & Samociuk 2006:79

Red flags in a process arise from anomalies on documents or transactions. Red flags on payment instructions being processed through a bank payment centre include the following:

- unusual delivery method of an instruction, for example through the mail or by courier with an urgent processing request
- unnecessary words or explanations on the request to make it appear more plausible
- appearance or style not consistent with normal transactions
- beneficiary name spelt incorrectly when compared with the account number
- payment not consistent with the normal business of the customer

Source: Iyer & Samociuk 2006:80

3.3.1.3 Recognising system red flags

System red flags arise from monitoring routines built into computer and communications systems. The following illicit behaviour can be detected (Iyer & Samociuk 2006:80):

- Someone logs onto the system using the user identification and password of an employee who is on leave, or attempts to log in if the password is disabled while the employee is on leave.
- There is a higher than average number of failed logon attempts.
- There are logons from areas outside the normal work area.
- There are logons at unusual times of the day.
- There is unusual network traffic.
- Control or audit logs are turned off.

3.3.1.4 Recognising corporate red flags

Many corporate failures around the world have been preceded by red flags. These were clear indications of the subsequent collapse. These red flags include

- investment analysts blacklisted by the company for writing negative reports
- concerns raised by regulators
- downgrading of the companies' credit rating
- solvency warnings by statutory accountants

Source: Iyer & Samociuk 2006:80

Potential corporate red flags indicating fraud, which are consistent with fraud perpetrated by senior management, include

- overzealous acquisition strategies without proper screening or due diligence
- autocratic management decisions around business relationships, such as a refusal to change a major supplier
- losses and declining margins on sales
- artificial barriers put up by directors to avoid answering questions
- excessive secrecy
- rumours and low morale
- complacent financial director
- overriding of budgetary controls
- discrepancies and deviations
- missing records or lack of detail
- unusual manual payments or adjustments
- consultants given a free rein

Source: Iyer & Samociuk 2006:80

ACTIVITY 3.1

1. Can you think of any more red flags?
2. What other indicators do you think there are of unusual or suspicious behaviour?
3. How would you deal with such indicators?

3.3.2 Whistle-blowing

Whistle-blowing simply means to report any irregularity, crime or transgression that a person may be aware of. This has to do with an internal matter in the workplace and may be either an internal or an external disclosure. Just taking note of some criminality or act of wrongdoing and reporting your observations or suspicions to a colleague over a cup of coffee during a lunch break does not constitute an act of whistle-blowing.

At some stage, most of us will have entered a public building and noticed posters placed at strategic locations declaring that the organisation (a certain public entity) has a "zero-tolerance" policy on fraud and corruption, and inviting you to blow the whistle, should you know of any such

activity. Usually a toll-free number is provided for making such reports. You may even have encountered a hotline or fraud reporting channel as part of the fraud risk management strategy or plan in the organisation you work for.

Whatever the case may be, you might have wondered what the terms "whistle-blowing" and "whistle-blower" entail; how this process works; what types of crimes, transgressions, unethical behaviour or conduct can be reported; and what the legalities are if a whistle-blower receives any protection or incentive. (Please also see paragraph 6 for a discussion on protected disclosures.)

Whistle-blowing requires some form of activity, usually in the form of a disclosure to a person in a position of authority. Simply taking mental note of the act of wrongdoing, asking the wrongdoer to desist from such activity or discussing the situation with colleagues without requiring or expecting any action to be taken does not constitute whistle-blowing (Miceli & Near 1992:16).

In some circles, whistle-blowing may be referred to as a "tip-off", while the person providing the "tip-off" is referred to as the whistle-blower. The term "whistle-blowing" is not defined in South African statutory law and, therefore, does not have any legal implication, other than describing the act or activity of blowing the whistle on perceived misconduct or observed unethical conduct.

According to Kloppers (1997:240– 241), whistle-blowing in general can be described as "the activity of disclosing information considered to be in the public interest". This would entail information about criminal activity, a contravention of any statutory requirement, improper or unauthorised use of public and other funds, miscarriage of justice, abuse of power, maladministration, and danger to the health or safety of any individual and any other misbehaviour or malpractice.

From a criminologist's perspective, "whistle-blowing is a pro-active strategy aimed at preventing crimes such as the various manifestations of fraud, embezzlement, corruption and employee theft".

The purpose of whistle-blowing is to provide a conduit or communication channel for employees to disclose wrongdoing or professional misconduct or fraudulent and unethical behaviour in the workplace (Joubert 2000:10).

Holtzhausen (2007:35), referring to Uys (2005) and Near and Miceli (1996), says that "whistle-blowers have two ways of reporting organizational wrongdoing, namely to authorities within the organization, or regulatory authorities outside the organization and therefore two main forms of whistle-blowing can be identified, namely internal and external whistle-blowing".

3.3.2.1 Internal whistle-blowing

Holtzhausen (2007:37), with reference to Johnson and Wright (2004), asserts that "internal whistle-blowing refers to reporting to people or managers within the organisation who are higher up in the organizational hierarchy. Those who receive internal complaints may be direct line managers, human resource representatives, chief executive officers, members of the executive council, or board of directors".

3.3.2.2 External whistle-blowing

Holtzhausen (2007:37), with reference to Miceli and Near (1994), says that "external whistle-blowing refers to the disclosure of information outside the organization and includes media, politicians, public protectors, government bodies, regulatory bodies and enforcement agencies".

(i) Standards and best practices in ethics or whistle-blowing hotlines

In the absence of legal provisions guiding the set-up of whistle-blowing hotlines, you may wonder if there are any standards or regulations for operating a "hotline". In South Africa, the Ethics Institute of South Africa has developed an External Whistle-blowing Hotline Service Provider

Standard, which is a best-practice set of guidelines or norms for professional and ethical conduct of external whistle-blowing hotline service providers.

You can obtain this service provider standard and more information regarding whistle-blowing from the Ethics Institute of South Africa, available at: http//www.ethics.org.

(ii) Whistle-blowing hotlines

A whistle-blowing hotline is one of the communication channels that enable members of the public or persons belonging to a particular organisation to lodge disclosures or make a report on perceived misconduct or observed unethical conduct in an anonymous or confidential manner.

One of the communications channels offered is a dedicated telephone number, usually toll-free and staffed by call centre operators. These dedicated telephone numbers are known by different names, such as

- hotlines
- ethics lines
- fraud call centres

Other communication channels offered include

- fax lines
- a postal address
- an e-mail address
- various websites

Examples of hotlines offered by South African public entities and government departments are as follows:

TABLE 3.2

Host organisation	**Dedicated number**	**Description**	**Activities that can be reported**
SARS	0800 00 28 70	SARS Hotline	Fraud and corruption
SIU	0860 748 748	SIU Corruption Hotline	Fraud and corruption in government
NPA	0800 21 25 80	NPA Service Delivery Hotline	Corruption and wrongdoings or transgressions in terms of the NPA values
SAPS	08600 10111	Crime Stop	Information about any crime, or any suspicious activities, or if you think you have useful information that may help prevent a crime or help the police in the investigation of a crime that has already taken place
Public Service Commission	0800 701 701	National Anti-Corruption Hotline (NACH)	Suspected acts of corruption in the public service

Examples of external whistle-blowing hotline services offered to stakeholders of client organisations are as follows:

TABLE 3.3

Host organisation	**Dedicated number**	**Description**	**Activities that can be reported**
KPMG	Client specific	KPMG Ethics Line	Client-specific activities
Deloitte	Client specific	Deloitte Tip-offs Anonymous	Client-specific activities

Some organisations have online information, informing employees and stakeholders of their hotline reporting mechanisms, for example

- http://www.kagisomedia.co.za/docs/KagisoMediaEthicsHotline.pdf
- http://www.parks-sa.co.za/about/crime/default2.php
- http://www.pggroup.co.za/news/news_View.asp?newsId=6
- http://www. mintek. co. za/full-pages. php? bus_cat=1db49810a48bba291e12d9e9ba79ca52&-guid=9d65b6805bbf43fa9f89d56d2d53f2ec&level=1

- http://www.mfanonymousreports.co.za/MutualAndFederal/HowDoesItWork.htm

The following are examples of types of disclosures of wrongdoing, professional misconduct, fraudulent and unethical behaviour that can be reported using hotlines:

- suspected contract irregularities and violations of procurement guidelines and policies
- corruption
- fraud
- bribery or acceptance of gratuities
- maladministration
- misuse of funds or assets
- misuse or abuse of company resources
- illegal disclosure of information
- acts of dishonesty
- ill treatment of members of the public or clients
- theft
- abuse of authority
- nepotism
- sexual harassment
- racism or discrimination
- unethical conduct

(iii) Websites

Most of the above-mentioned hotlines are supplemented by a reporting channel on a website hosted by the organisation providing the whistle-blowing hotline. These internet channels usually have a link to a report with fields in which the information is provided. In some cases, these internet forms are referred to as "suspicious activity reports". These forms can also be printed from the internet site, completed and posted or transmitted by fax to the organisation. An example of such a service is found on the website hosted by the South African Revenue Service (SARS), which can be found at http://www.sars.gov.za.

Under the heading Report a Suspicious Activity, the prospective whistle-blower is directed, via the link provided, to a form that can be completed.

According to the SARS website, a suspicious activity refers to "any conducted or attempted activity or pattern or display of transactions which are suspect or appear to give reason to suspect". Some typical examples would be as follows:

- a person or business being required to pay a certain type of tax, but not doing so
- a person or business employing people and deducting employees' tax from the employees, but not issuing IRP5 certificates to the employees
- a person or business being required to pay a particular tax, being registered as a taxpayer, but not submitting the required returns to SARS
- a person living beyond his/her obvious financial means or pursuing a particularly extravagant lifestyle in comparison with a person having similar levels of income
- a person found to be carrying an unusually large amount of currency in any form, while travelling in or out of South Africa
- a person who derives income from a criminal activity
- a person or business submitting fraudulent VAT refund claims
- a person or business liable to be registered for VAT, but not being so registered
- a person or business owing SARS money as a result of an assessment or schedule, but not paying SARS
- a person who is dishonest in a return or submission to SARS

3.4 STATUTORY REPORTING OBLIGATIONS

There are various legislative measures that aim to prevent and combat crime. These legislative measures impose statutory reporting obligations on certain categories of persons or institutions to report certain illegal activities or suspicions to specific authorities or persons in authoritative positions, using prescribed procedures.

We will now look at the statutory provisions that provide for crime-reporting obligations and the categories of crimes to which they apply.

3.4.1 Prevention and Combating of Corrupt Activities Act 12 of 2004

The Prevention and Combating of Corrupt Activities Act 12 of 2004 (PCCAA) is another example of government's attempt to prevent and combat crime and, more specifically, corruption.

The PCCAA provides for the offence of corruption and offences related to corrupt activities. More importantly, however, for the purpose of this chapter, the PCCAA imposes a legal duty on certain persons holding positions of authority to report certain corrupt transactions. These persons are referred to below.

Section 34(1) of the PCCAA provides as follows:

> Any person who holds a position of authority and who knows or ought reasonably to have known or suspected that any other person has committed –
>
> (a) an offence under Part 1, 2, 3 or 4, or section 20 or 21 (in so far as it relates to the aforementioned offences) of Chapter 2; or
>
> (b) the offence of theft, fraud, extortion, forgery or uttering a forged document, involving an amount of R100 000 or more, must report such knowledge or suspicion or cause such knowledge or suspicion to be reported to any police official.

3.4.1.1 Offences that must be reported

The offences that must be reported, referred to in section 1(a) of the PCCAA, are as follows:

- Chapter 2, Part 1 refers to the "general offence of corruption". The "general offence of corruption" is provided for in section 3 of the PCCAA, which reads as follows:

  Any person who, directly or indirectly –

(a) accepts or agrees or offers to accept any gratification from any other person, whether for the benefit of himself or herself or for the benefit of another person; or
(b) gives or agrees or offers to give to any other person any gratification, whether for the benefit of that other person or for the benefit of another person, in order to act, personally or by influencing another person so to act, in a manner –
    (i) that amounts to the –
        (aa) illegal, dishonest, unauthorised, incomplete, or biased; or
        (bb) misuse or selling of information or material acquired in the course of the, exercise, carrying out or performance of any powers, duties or functions arising out of a constitutional, statutory, contractual or any other legal obligation;
    (ii) that amounts to –
        (aa) the abuse of a position of authority;
        (bb) a breach of trust; or
        (cc) the violation of a legal duty or a set of rules;
    (iii) designed to achieve an unjustified result; or
    (iv) that amounts to any other unauthorised or improper inducement to do or not to do anything, is guilty of the offence of corruption.

- Chapter 2, Part 2 refers to offences in respect of corrupt activities relating to specific persons. These persons are
  - public officers
  - foreign public officials
  - agents
  - members of legislative authority
  - judicial officers
  - members of the prosecuting authority
- Chapter 2, Part 3 refers to offences in respect of corrupt activities relating to receiving or offering of unauthorised gratification by or to party to an employment relationship.
- Chapter 2, Part 4 refers to offences in respect of corrupt activities relating to the following specific matters:
  - witnesses and evidential material during certain proceedings
  - contracts
  - procuring and withdrawal of tenders
  - auctions
  - sporting events
  - gambling games or games of chance

From the above list, it is clear that the nature of the criminal conduct that must be reported is very wide.

3.4.1.2 Person liable to make a report

The PCCAA prescribes which persons are legally obliged to make a report in terms of the reporting duty created by the PCCAA.

In terms of section 34(1) of the PCCAA, any person who holds a position of authority who knows or reasonably ought to have known or suspected that any other person has committed any of the offences listed above, is legally obliged to make a report as prescribed.

According to the PCCAA, the following persons are regarded to "hold a position of authority", namely

(a) the director general or head, or equivalent officer, of a national or provincial department

(b) in the case of a municipality, the municipal manager appointed in terms of section 82 of the Local Government: Municipal Structures Act 117 of 1998
(c) any public officer in the senior management service of a public body
(d) any head, rector or principal of a tertiary institution
(e) the manager, secretary or a director of a company as defined in the Companies Act 61 of 1973, and this includes a member of a close corporation as defined in the Close Corporations Act 69 of 1984
(f) the executive manager of any bank or other financial institution
(g) any partner in a partnership
(h) any person who has been appointed as chief executive officer or an equivalent officer of any agency, authority, board, commission, committee, corporation, council, department, entity, financial institution, foundation, fund, institute, service, or any other institution or organisation, whether established by legislation, contract or any other legal means
(i) any other person who is responsible for the overall management and control of the business of an employer
(j) any person contemplated in the above categories who has been appointed in an acting or temporary capacity

3.4.1.3 Manner in which report must be made

The PCCAA prescribes that the report must be made to any police official and the PCCAA describes the manner in which the report must be taken down by the police official. Below is an example of the format prescribed in the PCCAA.

TAKING DOWN REPORT CONTEMPLATED IN SECTION 34 (3) (*a*) OF THE PREVENTION AND COMBATING OF CORRUPT ACTIVITIES ACT, 2004

TO: THE HEAD OF THE COMMERCIAL BRANCH: HEAD OFFICE, DETECTIVE SERVICE: CENTRAL REPORTING OFFICE
I, (full names and surname)
(rank)
(service number)
stationed at
a police official in the South African Police Service,
have received the following report
(*report attached, if applicable*)
from a person holding a position of authority as contemplated in section 34(4) of the Act,
(*full names and surname of person making the report*)
with the following contact particulars:
Contact address:
Telephone number:
Cellular phone number:

E-mail address:
Business/employment address:
Business telephone number:
Business e-mail address:
The report received entails the following:
Description of offence: (sections 3; 4; 5; 6; 7; 8; 9; 10; 11; 12; 13; 14; 15; 16; 20 or 21 of the Act **or** theft, fraud, extortion, forgery or uttering of a forged document involving an amount of R100 000,00 or more)
(Circle the applicable offence/s)
1. Description of the nature of the knowledge or suspicion of offence referred to above:
2. Name and contact details of person/s allegedly involved:
3. When did the offence/s occur or is it ongoing?
4. Any information to the reporter's knowledge about the standard of living of the person/s allegedly involved
5. Name and contact details of possible witnesses to the alleged offence/s:
6. Manner in which acknowledgement of receipt is preferred (only applicable in respect of facsimile, telephonic or electronic reports):
Signed at on this day of 20
SIGNATURE OF POLICE OFFICIAL TAKING DOWN THE REPORT
Unique reporting reference number (CAS number)
(To be inserted by the police official to whom the report is made. A corresponding number must appear on the acknowledgement of receipt (Annexure B))

The PCCAA further prescribes that the police official responsible for the report has to provide the person making the report with an acknowledgement of having received the report. An example of the format of the acknowledgement of the receipt of the report, as prescribed by the PCCAA, is shown below:

Unique reference number (CAS number)	
	(This receipt is not valid without this number)
ACKNOWLEDGEMENT OF RECEIPT IN TERMS OF SECTION 34(3)(a) OF THE PREVENTION AND COMBATING OF CORRUPT ACTIVITIES ACT, 2004 (ACT NO. 12 OF 2004)	
I, (full names and surname)	
(rank)	
(service number)	
stationed at	
a police official in the South African Police Service, hereby acknowledge receipt of a report	
received from	
(name)	
The following documentation has been received with the report:	
Signed at (place), on this day of 20	
	SIGNATURE OF POLICE OFFICIAL

Once the report has been received and the acknowledgement of receipt issued, the PCCAA further prescribes that the completed report must be faxed to the Head of the Commercial Branch: Head Office, Detective Service: Central Reporting Office. Once the report has been received, the Head of the Commercial Branch must ensure that an investigator of the Commercial Branch contacts the person who made the report and takes down a complete affidavit, which could serve as a basis for a police investigation into the report.

3.4.2 The Public Finance Management Act 1 of 1999

The Public Finance Management Act (PFMA) aims to

- regulate financial management in the national government and provincial governments
- ensure that all revenue, expenditure, assets and liabilities of those governments are managed efficiently and effectively
- provide for the responsibilities of persons entrusted with financial management in those governments
- provide for matters connected therewith

The PFMA can be seen as the cornerstone of corporate governance in the national and provincial governments. It prevents the abuse of the supply chain management system and provides that an accounting officer or accounting authority must investigate any allegations against an official or other role-player of corruption, improper conduct or failure to comply with the supply chain management system, and when justified, report any conduct that may constitute an offence to the South African Police Service.

In addition to detection processes and controls, organisations may be also use data analysis, continuous auditing techniques and other technology tools to effectively detect fraudulent activity.

Proactive consideration of how certain fraud schemes may result in identifiable types of transactions or trends enhances an organisation's ability to design and implement effective data analysis. Data analytics can also be used to ensure the effectiveness of other fraud preventive and detective controls cost-effectively.

Although it does not form part of this module, continuous auditing is the use of data analytics on a continuous or real-time basis, thereby allowing management or auditing to identify and report fraudulent activity more rapidly. For example, a so-called **Benford's Law analysis** can examine expense reports, general ledger accounts and payroll accounts for unusual transactions, amounts or patterns of activity that may require further analysis. This is a quick, high-level tool used in auditing large pools of data. What it does is to show digits from unusual transactions that follow a definite pattern. These digits are then compared with a sample from a similar, fraud-free account. If the pattern corresponds with the pattern from the fraud-free account, there does not appear to be anything wrong. However, if the patterns differ, it may indicate an irregularity (Stalcup 2010).

Similarly, continuous monitoring of transactions subject to certain "flags" may promote quicker investigation of higher-risk transactions.

Technology-based tools enhance the ability of management at all levels to detect fraud. Data analysis, data mining and digital analysis tools can

- identify hidden relationships among people, organisations and events
- identify suspicious transactions
- assess the effectiveness of internal controls
- monitor fraud threats and vulnerabilities
- consider and analyse thousands or millions of transactions

Some auditors and consulting firms have developed tools as part of their fraud detection efforts that analyse journal entries to mitigate management override of the internal control system. These tools identify transactions subject to certain attributes that could indicate risk of management override, such as user identification, date of entry and unusual account pairings.

Evidence of fraud can sometimes be found in e-mails as well. The ability of an organisation to capture, maintain and review the communications of any of its employees has led to the detection of numerous frauds in the past. This is accomplished through the use of strict and regular backup programs that capture data, not with the intent of uncovering fraud, but merely as a safeguard in the event that a retrospective search for evidence may be necessary.

As organisations grow and technology needs change, so do the opportunities for fraud. Because fraud and misconduct schemes cannot all be fought with the same tools and techniques, the organisation will periodically need to assess the effectiveness of process controls, anonymous reporting and internal auditing.

3.5 AUDITING

Organisations can never entirely eliminate the risk of fraud. There are always people who are motivated to commit fraud, and an opportunity can arise for someone in any organisation to override a control mechanism or collude with others to do so.

The Association of Certified Fraud Examiners (ACFE 2008) defines fraud auditing as "a proactive approach to detect financial frauds using accounting records and information, analytical relationships, and an awareness of fraud perpetration and concealment schemes".

3.5.1 Areas in which fraud may be detected

By using these techniques, auditors can detect fraud and other crimes in the following areas of an organisation's operations or relationships with business partners or clients:

- **The owners, corporate controllers or managers.** From the perspective of creditors, shareholders and regulators, examples include theft of company assets, insider trading and fraudulent financial reporting.
- **Customers/clients.** From a customer/client perspective, examples include misleading advertising, price fixing, short deliveries, false statements of accounts, false claims in respect of the specification of products or services and investment fraud. From a business's perspective, examples include theft, cheque fraud, credit card fraud, obtaining credit under false pretences, false claims and identity fraud.
- **Government.** From a government perspective, examples include regulatory transgressions, tax evasion, VAT fraud, customs fraud, false claims and statutory non-compliance.
- **Insurance.** An example is false insurance claims for loss or damages.
- **Employees.** From the perspective of employers, examples include false expense accounts and travel claims, employee theft, corruption, IT systems abuse and security transgressions, confidentiality breaches, selling of trade secrets and industrial espionage. From the perspective of employees, examples include labour law transgressions, non-payment of UIF, non- payment of PAYE and statutory non-compliance with occupational health and safety regulations.
- **Vendors, suppliers and consultants.** From a business's perspective, examples include short deliveries, double invoicing, false invoices, inflated invoices, corruption and procurement fraud.
- **Competitors.** From the perspective of competitors, examples include theft of trade secrets, corruption and unauthorised access to data.

  Shareholders and creditors. From the perspective of shareholders and creditors, examples include false financial statements, reckless and fraudulent management, insider trading and criminal insolvency.

Fraud auditing focuses on activities and techniques that promptly detect whether fraud has occurred or is occurring. Detection techniques used by auditors should be flexible, adaptable and continuously changing to meet the various changes in risk. Important detection methods include

- recognising red flags
- an anonymous reporting mechanism, such as whistle-blower hotlines
- suspicious activity report mechanisms
- process controls
- proactive fraud detection procedures

3.5.2 Process controls

Process controls that are specifically designed to detect fraudulent activity include

- reconciliations
- independent reviews
- physical inspections
- physical counts
- analyses
- audits

Source: (ACFE 2008:367)

3.5.3 Proactive fraud detection procedures

To detect fraudulent activity, organisations can use data analytics, continuous auditing techniques and other technology-based tools, such as data analysis, data mining and digital analysis.

3.5.4 Data analytics

The widespread use of computers in organisations and businesses has resulted in an abundance of data. And since most operations, accounting, payroll, vendor, procurement and human

resource management systems in organisations have become automated, more information in electronic format is available for examination. The use of computer-based communications has also grown rapidly, with the result that electronic information can be stored on personal computers and other electronic devices. These devices can provide evidence or indications of the commissioning of an offence. Many of these devices communicate or receive and send data messages through the servers of the organisations that employ the user.

3.5.4.1 Definition of "data analytics"

Data analytics is also referred to as data mining, digital analysis, database reporting, data analysis and data interrogation. In general, it can be defined as the "automated extraction of hidden predictive information from databases"[1]. Data analysis refers to the use of technology to identify anomalies, trends and risk indicators within large populations of transactions.

3.5.4.2 Definition of "continuous auditing"

Continuous auditing is the use of data analytics on a continuous or real-time basis, thereby allowing management or auditing to identify and report fraudulent activity more quickly. For example, a Bedford's Law analysis (see paragraph **4.2** above) can examine expense accounts, general ledger accounts and payroll accounts for unusual transactions, amounts or patterns of activity that may require further analysis. Continuous monitoring of transactions that can indicate red flags may lead to quicker detection (ACFE 2008:36).

3.5.4.3 Use of technology to perform data analysis

Data analysis uses technology to identify irregularities, trends and risk indicators within large volumes of transactions. Users of this technology can examine journal entries to search for suspicious transactions that occur at the end of a period or for those entries that were made in one period and then reversed in the next period so that the books appear to balance. Data analysis also enables users to identify relationships among people, organisations and events. The technology referred to in this context is also known as "technology tools" and includes

- data analysis tools
- data mining tools
- digital analysis tools

These tools may also allow users to look for journal entries posted to revenue or expense accounts that improve net income to meet analysts' expectations or incentive compensation targets. Moreover, data analysis allows users to identify relationships among people, organisations and events (ACFE 2008:36–37).

3.6 PROTECTED DISCLOSURES

Probably the most important issue that arises with whistle-blowing or tip-offs is that of anonymity and protection against harm, reprisal, victimisation or intimidation. We may be inclined to think that an organisation would respond positively to a report of corruption or wrongdoing, but often just the opposite occurs and there is a so-called witch-hunt to identify the person who reported the wrongdoing and to act against him/her.

ACTIVITY 3.2

1. Find an example where disciplinary action was taken against a whistle-blower. What were the reasons for taking such action and what was the result?
2. How would you deal with information that pointed to a protected disclosure?

1. This definition is found in several publications, but the primary source is not acknowledged or credited.

3. Refer to the PDA and make a list of what you would do.

If whistle-blowing is to have any impact on preventing and reducing fraud and corruption in South Africa, the government needs to respond by providing some form of statutory protection measures to protect whistle-blowers against reprisal.

In this regard, the South African legislature responded by promulgating the Protected Disclosures Act 26 of 2000 (PDA). The objective of the PDA is as follows:

(a) To make provision for procedures in terms of which employees in both the private and the public sector may disclose information regarding unlawful or irregular conduct by their employers or other employees in the employ of their employers;
(b) to provide for the protection of employees who make a disclosure which is protected in terms of this Act;
(c) and to provide for matters connected therewith.

The objectives of the PDA are therefore threefold (Holtzhausen 2007:43):

- It aims to provide for procedures in terms of which an employee can, in a responsible manner, disclose information regarding improprieties committed by his or her employer.
- It protects an employee, whether in the private or public sector, from being subjected to occupational detriment on account of having made a protected disclosure.
- It provides for certain remedies in connection with any occupational detriment suffered on account of having made a protected disclosure.

In quoting the Open Advice Democracy Centre, Holtzhausen (2007:40) states that the PDA should play a central role in the overall fight against corruption and that it aims to promote a safe environment in which someone who suspects or knows in good faith that something is wrong, reports it to a relevant authority that has the power to, for example, investigate the matter and, if able, remedy the situation. According to Holtzhausen (2007:40–41), the PDA should create a safe legal environment for disclosures and therefore create a culture where the disclosure will be heard in a responsible manner and the messenger treated with respect, thus promoting the eradication of crime and misconduct in organs of state and private bodies. The PDA is informally known as the "Whistle-blower Act" (Holtzhausen 2007:66).

According to Holtzhausen (2007:42), the PDA is specifically structured in a way that best serves the interest of accountable organisations. It is important to note that only *after* internal reporting channels have been exhausted or fail are disclosures to external bodies protected. This means that the disclosure must be made according to the procedures provided for in the PDA.

For your purposes as students, the most important issues covered by the provisions in the PDA are as follows:

- concepts and definitions, such as "disclosure", "employee", "employer", "impropriety", "occupational detriment" and "protected disclosure"
- the objectives and application of the PDA
- an employee making a protected disclosure may not be subjected to occupational detriment by the employer
- legal remedies
- protected disclosure to a legal advisor
- protected disclosure to an employer
- protected disclosure to a member of Cabinet or Executive Council
- protected disclosure to certain persons or bodies
- a general protected disclosure
- regulations issued in terms of the PDA

In order to invoke the protection afforded by the PDA, the disclosure to bodies other than the channels provided by the employer should be made only in terms of the prescribed procedures.

Whistle-blowers would be wise to familiarise themselves with the provisions of the PDA to understand that the nature of the disclosure determines whether it is a protected or an unprotected disclosure.

In terms of sections 5–9 of the PDA, a disclosure must be made in one of five ways in order to be protected:

- to a legal representative
- to an employer
- to a member of Cabinet or Executive Council
- to a specific person or body
- as a general protected disclosure

Section 3 of the PDA provides that no employee may be subjected to occupational detriment by his or her employer on account, or partly on account, of having made a protected disclosure.

Investigators who discover crimes under circumstances that may relate to a protected disclosure are advised to refer to the PDA and ensure that they are aware of how this Act is applied.

3.7 SUMMARY AND CONCLUSION

The preceding discussion showed that investigations don't just happen by chance. Usually an event or discovery initiates an investigation. That event might be in the form of a report received by the police or the ethics department of a business enterprise. Alternatively, it may be as a result of a tip-off regarding suspected criminal activity received by a call centre operator via the fraud hotline of a government department, law enforcement agency or an ethics officer of a business enterprise. Investigations are also instituted to investigate a phenomenon or an occurrence such as a plane crash disaster.

It is clear that there are numerous ways in which to uncover a crime or a transgression. These include the use of red flags, auditing and other forms of analysis. But investigators should take note that, in certain instances, there is legislation regulating such activities. For instance, certain people may be expected to provide information, and their failure to do so may amount to an omission in terms of the legislation.

Chapter 4

Transgressions, non-compliance and dealing with stakeholders

Contents

4.1 INTRODUCTION

In the workplace, there are a number of ways in which an employee may be guilty of violating a policy or procedure that has been laid down to regulate the smooth operation of the organisation. There are many terms used to describe such acts: contraventions, infringements, misdemeanours, violations, neglect, misbehaviour, misconduct, transgressions, malfeasance, nonfeasance and misfeasance. Whatever words are used, they all describe some kind of irregular action on the part of the employee. It is not the object of this paragraph to deal with what these words mean, but just to make you aware of them so that you will know what they refer to when you do encounter them.

In this chapter we look at different transgressions and non-compliance. It is worth noting that the focus will be on labour relations issues. As forensic investigators, we are often expected to investigate an internal matter. It is therefore important that we understand the different transgressions and forms of non-compliance with policies that can be perpetrated by the employee.

In this chapter we will also reflect on two main stakeholders in investigations. The first stakeholder is the trade unions, which are often involved when the employees of an organisation are being investigated. It is very important for forensic investigators to be able to handle the trade unions. Perhaps the most important justification for the involvement of trade unions is to ensure that the investigation is not performed arbitrarily and that the rights of the employees are not violated during the investigation process. We will also look at how investigators should handle the media, which is the second stakeholder in the investigation process. It is worth noting that while the media can assist the investigation, any improper handling of information by the media can ruin the investigation.

4.2 TRANSGRESSIONS

In the labour context, a transgression is regarded as misconduct. There is a difference between a transgression and non-compliance, because misconduct is regarded as being more serious than non-compliance. Grogan (2009:52) states that

> "any misconduct that renders the continuation of the employment relationship intolerable or unworkable or that undermines trust and confidence between the employer and the employee is regarded as sufficient to justify dismissal ... Misconduct may have a bearing on the employment contract if committed either before or after the parties enter into the agreement and may, in appropriate circumstances, constitute a ground for dismissal."

Misconduct is one of three grounds recognised by the LRA to justify the dismissal of an employee. The others are incapacity and operational requirements. Misconduct is something that an employee can be held accountable for, while an employee cannot be held accountable for incapacity due to old age or becoming technologically challenged.

Dismissal on the grounds of misconduct is the ultimate sanction in the workplace and, therefore, the courts have developed the following two principles when dealing with issues of dismissal:

- Was there a good reason to dismiss?
- Did the employer follow a fair procedure before deciding on dismissal?

These two principles are subject to the following standards:

- The reason for the dismissal must not be classified as being automatically unfair.
- There must be a valid reason for the termination of the contract.
- The dismissal must be effected in a procedurally fair manner.

4.3 NON-COMPLIANCE

Compliance in this context means the adherence to requirements. Grogan (2009:124) uses the example of labour inspectors that have the authority to enter and inspect employers' properties and documents to ensure that they have complied with the requirements of the law with regard to consultation with employees. They may issue compliance orders to the employer to adhere to the requirements of the legislation, failing which they will face an order from the Labour Court. The penalties that a non-complying employer may face include the cancellation of state contracts, being prohibited from receiving state contracts in future, as well as substantive fines ranging between R500 000 and R900 000 (Grogan 2009:126).

4.4 DEALING WITH TRADE UNIONS

Dealing with trade unions is not normally the responsibility of a corporate or other investigator. This is normally handled by the human resource manager, who will be involved in the negotiations with the union representative.

Section 12(1) of the Labour Relations Act 66 of 1995 (LRA) provides that office bearers or officials of sufficiently representative trade unions may enter the employer's premises to "recruit members or to communicate with members, or otherwise serve members' interests". They are also entitled to hold meetings with employees outside their working hours at the employer's premises. Members of representative trade unions may also vote at their employer's premises in elections or ballots provided for in their union's constitution. The exercise of these rights is subject to "any conditions as to time and place that are reasonable and necessary to safeguard life or property or to prevent undue disruption of work".

It is when these rights are being exercised that the role of the corporate security officer or investigator becomes important. This person has the responsibility to safeguard the employer's premises and to ensure that meetings are held in accordance with the agreements between the

parties. If there are any compelling reasons why this is not possible, these are to be made known to the human resource manager so that he/she can take this up with the union/s.

In workplaces with more than 10 employees, members of the majority trade union are entitled to elect representatives, called "shop stewards". Their functions are to assist and represent members in grievance and disciplinary hearings, as well as monitoring the employer's compliance with labour legislation and collective agreements and reporting contraventions to the responsible authorities. They are entitled to take "reasonable" time off, with full pay, to perform these duties. If they exceed this or abuse their powers by intimidating non-members, disciplinary action may be taken against them (See *Independent Municipal & Allied Trade Union & others v Rustenburg Transitional Council* (2000) 21 ILJ 377 (LC).) (Grogan 2009:320).

If this does take place and you are requested to do the investigation, you must remember that any actions that you take will be challenged by the trade union, as your actions will be seen as an attempt by management to intimidate or place the shop steward in a bad light. Therefore, ensure that the integrity of your investigation is beyond reproach.

Although the LRA provides that a person does not commit either a delict or a breach of contract by taking part in or organising a protected strike, this immunity does not extend to conduct that otherwise amounts to an offence (Grogan 2009:38). The right to strike involves merely the right to withdraw labour and to picket peacefully. Unfortunately, it does happen that during strike action, some employees damage the employer's property or intimidate and assault workers who are not participating in the strike action. When this happens, it becomes the investigator's responsibility to investigate the matter and to identify the culprits. There are a number of ways in which this can be done effectively. The most obvious is to have a video recording made of the transgressors in action and then, should they have acted outside the protection of the strike action, to take action against them. This entails interviewing persons, identifying the persons involved and determining exactly what took place.

Investigation relating to labour unions – hereafter referred to as "trade unions" – is a specialised field and cannot be adequately addressed in a few pages. I will therefore confine this discussion to a few points that may be of importance. It is strongly recommended that when you are faced with any issue relating to labour issues in the workplace, you consult with an expert in the field.

The LRA recognises and provides for the formation and registration of three kinds of institutions to represent employers and employees in the collective bargaining process. These are

- trade unions
- employers' organisations
- workplace forums

4.4.1 Definitions

> A **trade union** is defined as "an association of employees whose principal purpose is to regulate relations between employees and employers, including any employers' association" (s 213 of the Labour Relations Act 66 of 1995). The primary function of a trade union is to engage in collective bargaining with their members' employers and to represent their members in grievance and disciplinary matters.

Every employee has the right to join and become a member of a union, irrespective of seniority. This is in contrast to a workplace forum, where senior employees/managers are excluded from being members. Where an employee's membership of a union causes a conflict of interest, that employee owes a duty of fidelity to the employer. If that employee's union activities and allegiance to the trade union causes incapacity or prevents him or her from discharging his or her duties as an employee, he/she may face dismissal for incapacity.

When an employee joins a trade union, he or she enjoys all the rights of membership, which includes collective bargaining.

> **Collective bargaining** is the process by which employers and organised employees seek to reconcile their differences through a process of making demands and concessions to reach an agreement. This is a difficult process because the parties must find common ground, which may require fixed positions to be abandoned.

The first step in a collective bargaining relationship is for an employer to recognise a registered trade union as the bargaining agent for its employees. This registered trade union must also represent a sufficient number of workers on the staff of the employer (Grogan 2009:340). When a decision has to be made in this regard, it must be noted that only a registered trade union that enjoys the majority status in the workplace – either independently or in coalition with another union – may negotiate agreements (Grogan 2009:349). A recognition agreement is then drawn up, which sets out the structures through which bargaining takes place.

Unions may represent their members in legal proceedings, which involve both civil and labour courts. Trade union officials are entitled to represent members in arbitration proceedings and also in the Labour Court, provided that they conform to the rules and procedures of the court (Grogan 2009:315).

> An **employers' organisation** is "any number of employers associated together for the purpose, whether by itself or together with other purposes, of regulating relations between employers and employees or trade unions" (Grogan 2009:327). Employers' organisations are therefore the employer's counterpart to trade unions. "Accordingly, the general rights accorded to trade unions in so far as they are applicable as well as the rights of individuals to belong to trade unions, apply *mutatis mutandis* to employers in respect of employers' organizations" (Grogan 2009:327).

Nothing prevents employers from grouping together on a non-statutory basis for the purpose of collective bargaining. According to Grogan (2009:328), nothing prevents them from forming federations that have *locus standi* to bring actions in their own names. Officials of employers' organisations are also entitled to represent their members in proceedings before the CCMA and the Labour Court, provided that the employers' association is bona fide.

Subcontracting on a limited scale is allowed, provided that it does not lead to a complete takeover of the employers' organisation. This means that representing the employer in CCMA or bargaining council proceedings is allowed, provided that the subcontractor does not deal with all the organisations' labour issues. If this does happen, it is regarded as a fraud on the register (Grogan 2009:328) and the employers' organisation may be deregistered (*National Employers' Forum v Minister of Labour & others* [2003] 5 BLLR 460 (LC)).

> A **workplace forum** is "(an) instrument (s) for promoting participative management through information-sharing, consultation, and joint decision making" (Grogan 2009:330). Workplace forums differ from trade unions in that they are charged with promoting the interests of all employees in the workplace and not just those of members of trade unions. The members of a workplace forum consist of workers and exclude senior managers. The members are nominated either by any registered trade union that has members in the organisation or by a petition signed by 20 per cent of the workforce, or 100 employees – whichever number is smaller.

The consultation referred to above is set out in section 85 of the LRA as follows:

(1) Before an employer may implement a proposal in relation to any matter referred to in section 84(1), the employer must consult the workplace forum and attempt to reach consensus with it.
(2) The employer must allow the workplace forum an opportunity during the consultation to make representations and to advance alternative proposals.
(3) The employer must consider and respond to the representations and alternative proposals made by the workplace forum and, if the employer does not agree with them, the employer must state the reasons for disagreeing.

(4) If the employer and the workplace forum do not reach consensus, the employer must invoke any agreed procedure to resolve any differences before implementing the employer's proposal.

ACTIVITY 4.1

Explain the differences between trade unions, employers' associations and workplace forums.

4.4.2 Code of good practice

The LRA requires that any relevant code of good practice be taken into account when considering whether dismissal was for a fair reason. The principal codes of good practice deal with the following:

- dismissal generally
- dismissal for operational requirements
- dismissal for sexual harassment

Source: (Grogan 2009:168)

The code of good practice should not be confused with the grounds for dismissal recognised by the LRA to justify the dismissal of employees, namely

- misconduct
- incapacity or poor work
- operational requirements

Source: (Grogan 2009:201)

It is quite likely that your investigation into allegations of misconduct will be the motivating factor for management to make a decision on what action to take against the person involved. You are unlikely to become involved in the investigation of allegations of incapacity, poor work or operational requirements, as this is the domain of senior management.

The method for the investigation of misconduct depends on the nature of the allegation. There are numerous classes of misconduct, ranging from absenteeism to unauthorised use of property. Your investigation will therefore concentrate on the nature of the allegation, taking into consideration that the burden of proof in a disciplinary matter is on a balance of probability. This means that, unlike in a criminal investigation where you have to prove the guilt of the accused beyond all reasonable doubt, in a disciplinary matter, you need only show that the defendant is guilty on a balance of probability. If we had to express this in percentages, it would mean that in a criminal case, the guilt of the accused has to be proved more than 95%, whereas 51% proof would be sufficient in a disciplinary matter.

Item 7 of the Code of Good Practice on Dismissals determines as follows:

> Any person who is determining whether dismissal for misconduct is unfair should consider -
>
> (a) Whether or not the employee contravened a rule or standard regulating conduct in, or of relevance to the workplace; and
> (b) If a rule or a standard was contravened, whether or not –
>
> (i) The rule was a valid or reasonable rule or standard;
> (ii) The employee was aware, or could reasonably be expected to have been aware, of the rule or standard;
> (iii) The rule or standard has been consistently applied by the employer; and

(iv) Dismissal with (*sic*) an appropriate sanction for the contravention of the rule or standard.

Source: Grogan 2009:203

The offence has to be proved and you will have to prove that the rule existed and that the employee broke it. Proof is usually done by way of the employee's contract or a collective agreement or the disciplinary code. The rule need not exist in written form because it is generally agreed that, for instance fraud and theft, would destroy the employment relationship between the parties. It is then generally assumed that the employee knew or should have known that his or her conduct could lead to dismissal.

In some instances, the employee may deny knowledge of this. It is then up to you to prove that the employee knew, or should have known, about it. This could be done by showing that the employee was present during a training session where this was dealt with – usually an induction course. The attendance list will usually be sufficient evidence.

In the workplace, there are also examples of mass dismissal for various reasons that range from failure or refusal to disclose the names of perpetrators to shrinkage of stock (Grogan 2009:205). In such cases, proof creates a special problem because you have to show that, on a balance of probabilities, each individual was involved, before action can be taken.

As far as the reasonableness of the rule is concerned, you simply have to show that it is operationally justified – in other words, that it promotes the employer's business and that it does not place an unreasonable burden on the employee.

The next requirement – that the rule was consistently applied – is satisfied by showing that previous contraventions by other employees have had the same result. If certain transgressors in the past were given final warnings for specific contraventions, this should be consistently applied. This means that unless there are other factors involved, persons should not later be dismissed for the same thing.

The last requirement, namely that the sanction be appropriate, is regarded by Grogan (2009:208) as "being the most problematic". A number of factors, such as provocation, previous employment history, length of service and the consequences of the particular infraction, should be considered. Although these are issues to be considered by the presiding officer, it remains your responsibility to present evidence to show the seriousness of the actions of the person involved.

ACTIVITY 4.2

1. Make a list of transgressions for which the sanction is dismissal on the first occasion and where warnings may be given. You should be able to get this information from your organisation's disciplinary code.
2. Are there other transgressions that you feel warrant instant dismissal? If so, what are they?

4.5 THE MEDIA

The media is a tool that investigators can use to receive assistance in investigations. In this regard, the media is extremely helpful in providing information both to and from the public. Nevertheless, because sensationalism sells newspapers, many reporters are after what they refer to as a "scoop". This sensational item will place them at an advantage over other newspapers because they "broke" the story first. All investigators need to be aware of the ulterior motives that some reporters or journalists may have and, therefore, be on guard when dealing with them. Many organisations have a communications or liaison department that deals with the press and issues press statements. This department consists of specially trained personnel that have the authority to deal with the press and issue statements.

Apart from these liaison departments, organisations also have a policy with regard to dealings with the press. They determine the name of a person with whom the press must deal, as well as what the form and content of the contact should be. This person is referred to as the liaison officer and he or she is the person that will contact you with regard to information about an investigation or incident in the workplace that you may be aware of.

In many cases, the investigation may be *sub judice* and any premature leaking of information could jeopardise your investigation or compromise a witness or witnesses. It is therefore suggested that you give the liaison officer sufficient information, without disclosing confidential information, and inform them that the matter is still being investigated and that further information will be communicated at some time in the future.

Beware of reporters who ask you for information "off the record"; there is no such thing. The information that you give will usually be published in some form or another, and you will be highly embarrassed if a subsequent investigator points a finger at you for being the source of the information. You may even face disciplinary action. It is preferable to deal with media requests in writing. Once you have received the request for information, draft an answer and forward it to the communications/liaison department. The advantage of this is that you then have the request, as well as the answer, on record and cannot be held responsible for any misinformation that has been printed.

It may even happen that you are approached by a television station for an interview. Make sure that you obtain official approval and that you are assisted by a liaison officer in such cases. Be particularly careful of what you say while being interviewed because it may happen that you are asked a question that may have serious repercussions in a court of law; it will be extremely difficult to explain what you said when faced with a recording in court.

ACTIVITY 4.3

Determine your organisation's policy on media matters and determine who your local liaison officer is.

4.6 SUMMARY AND CONCLUSION

Although there could be some differences between the objectives and purpose of investigations that happen outside the organisation and those that happen inside the organisation, the manner in which evidence is obtained remains the same. The rights that are accorded the suspects in external investigations are similar to the rights of the employees who are suspected of an internal transgression or non-compliance. This means that if evidence is not properly obtained, the organisation may be unable to deal with the said transgression or non-compliance.

In conclusion, not all investigators are fortunate enough to have the backing of legislation that allows them to obtain information; sometimes they have to use methods that are cumbersome and do not provide the desired outcome. Those investigators that can rely on legislation and official powers to do their work must do so strictly in accordance with the legislation. In this context, the investigators will be required to know and fully comprehend the labour legislation. If they contravene the provisions of the legislation, their credibility will be affected and the investigation may be ruined. Furthermore, investigators should not become complacent as far as labour legislation is concerned by assuming that employee transgressions and non-compliance lie within the domain of HR managers and will be dealt with by the latter.

Chapter 5

The case docket and investigation file

Contents

5.1 INTRODUCTION

The record of every investigation that is undertaken – whether by an official organisation such as a police service, a corporate investigator or a private investigator – must be contained in a file of some sort. Organisations have their own unique names for these files. The South African Police Service uses the term "case dockets", while other organisations merely call them "files" or

"investigation files". For the purpose of this module, I will refer to these files as case dockets or dockets.

These dockets contain all the information collected during an investigation and are the single most important source of evidence that may be used to determine whether a prosecution will take place or not. These dockets must be structured logically so that the contents are readily available when a decision is to be made – either by a public prosecutor or a disciplinary officer. If a person who is unfamiliar with a docket has to search through it to find what is required, it will waste valuable time.

The South African Police Service has particular requirements regarding the arrangement of case dockets, and the same is true of other organisations. Generally speaking, witnesses' statements, forensic reports and documentary evidence are kept separate from ordinary reports, letters and other documents that will not be used as evidence.

There is usually some form of an investigation diary, which is a record of what has been done in the investigation. This investigation diary is very important. Its value is often underestimated because many investigators believe that their memories are good enough to remember the details of an investigation – until they get to court and have problems explaining events that happened a long time ago.

Moreover, if you are unable to continue with an investigation or become unavailable for some or other reason, a proper record of all actions taken during the investigation will allow subsequent investigators to take over the investigation from you.

5.2 STRUCTURE OF A CASE DOCKET

A docket should be structured in such a way that the investigator is able to find a particular document easily, without having to search through a haphazard collection of papers. This means that those documents that contain evidence of some kind must be kept to one side so that they are not lost or destroyed. Of particular importance are witness statements. These are sometimes referred to as the "building blocks" of an investigation. They are of great importance because they form the basis of the case against the accused or the defendant.

Many investigators do not appreciate the importance of safeguarding witness statements against loss, destruction, theft and contamination. Like any other evidence, these statements should be kept in the condition that they were in when they were recorded. For example, consider the following scenario: A witness has made a handwritten affidavit. The investigator, a neat and precise person, prefers to have his statements typed. Therefore, when arriving back at the office, he has the statement typed up and then either destroys the original handwritten copy or returns it to the witness, as per the witness's request. At some point in the investigation, the investigator needs the signed original, so he requests the witness to return it to him. However, the witness refuses to hand over the original copy or to sign the typed copy. Although there is a concept known as "the best evidence rule", which makes provision for a court to accept a copy of a document if the original has been lost, it applies only when the case is before the court. An unsigned copy will never be accepted for administrative judicial purposes, such as for the issuing of a warrant of arrest or for a search and seizure.

A further example is where a witness testifies in court and deviates substantially from her statement so that it becomes necessary to declare her a hostile witness and to confront her with her handwritten and signed original. If the original cannot be produced, there will be no evidence to discredit the witness and the case may be lost. The same applies when a person is to be charged with perjury, that is, for making two conflicting statements under oath or for making a single false sworn statement. In all these cases, you will need the original statements as documentary evidence.

The docket is best divided into various parts. The SAPS uses an alphabetical system from A to C. The "A" section contains all the evidential material, the "B" section contains all the correspondence, and the "C" section contains the investigation diary. Other organisations may have their own unique requirements to suit their own particular purposes, so it is best to develop a practical yet uncomplicated system that does not cause confusion. Always remember that you are not the only person that will be dealing with the docket, so it must be straightforward and easily understood by people without forensic experience.

The different sections in the docket must be clearly indicated by means of dividers so that the reader is not confused. Note that your docket may consist of a lever arch file; you need not use a specially designed docket cover like that used by the police. Also mark the contents of the docket sequentially, starting from "one" in each section, so that if you refer to a particular document in your investigation diary, you merely have to refer to the number and the section where it has been filed. It may also be very useful to cross-reference documents that refer to other documents. If a witness makes a supplementary statement, this should be indicated in the first statement so that the reader is aware that there is an addendum. However, BEWARE of conflicting statements, as this will make your witness a suspect and cast serious doubt on your case.

5.3 INVESTIGATION FILE

An investigation file is the same as a case docket in so far as it contains a record of the investigation in the form of statements, reports sent and received, as well as correspondence and other relevant documentation. It could also contain some form of a diary that indicates what has been done in the investigation. Such a file – especially one used by private investigators – also contains full particulars of all costs incurred, as well as payments received.

The structure of such a file varies according to the policies or requirements of the organisation concerned. It is therefore not possible to lay down hard-and-fast rules for how they are to be structured. The only requirement is that such a file should contain a complete record of the investigation, as well as the result. Bear in mind that these files form part of budgetary control and may be audited.

5.4 REPORTS

According to English (2006:147), there are various types of investigative/forensic reports, which are related to other kinds of written messages found at college, university, in business and in industry. They are related in format, style and approach to the following:

- theses
- business proposals
- business plans
- minutes
- instructions
- technical descriptions

For the purpose of this module, I will confine myself to discussing only investigative or so-called forensic reporting.

Reports of this nature not only form the basis of what has been done, but also contain findings and recommendations for management to act upon. Reports are informative in the sense that they may describe what has been done during an investigation, the process followed, the findings and recommendations. If there is a systemic deficiency in the investigation, it may be pointed out in a report, along with recommendations for corrective measures to be taken.

5.4.1 Definition of an investigative report

Van Rooyen (2001:82) defines an investigative report as "a communication of information set forth in an accurate, concise, clear and complete manner serving as a record of a given incident".

5.4.2 Requirements for a good report

Van Rooyen (2001:83) lists the following as requirements for a good report:

- *Completeness*. This means that there is nothing missing from the report.
- *Accuracy*. An exact, precise and reliable rendition is given of the activity or crime.
- *Factual*. This refers to experiences and occurrences that the reporter has experienced first-hand.
- *Hearsay*. This refers to second-hand information that the reporter has heard from others.
- *Meaning of words/Comprehension*. The reporter must use the correct words to describe what has to be said. Under no circumstances should flowery or ambiguous language be used, which would be open to different interpretations.
- *Timeliness*. The report must be submitted within the timeline set by the client, or in time for the recipient to be able to act upon it. (In the motor manufacturing world, this is referred to as the "just in time" principle, which means that the right part must be available at the right time so that the assembly line is not kept waiting.)
- *Objectivity*. The report must not be influenced by the feelings of the reporter. Facts should be stated as they are, and not as the reporter would have liked them to be; opinions are reserved for later in the report.
- *Referencing*. Refer to previous reports, if necessary, so that the reader is aware that there is a history to be considered.

5.5 REPORTING

Reports differ according to the situation. Although we are concerned here with investigative reporting, it is important to note that all reports have one thing in common: they require either a decision to be made or some action to be taken.

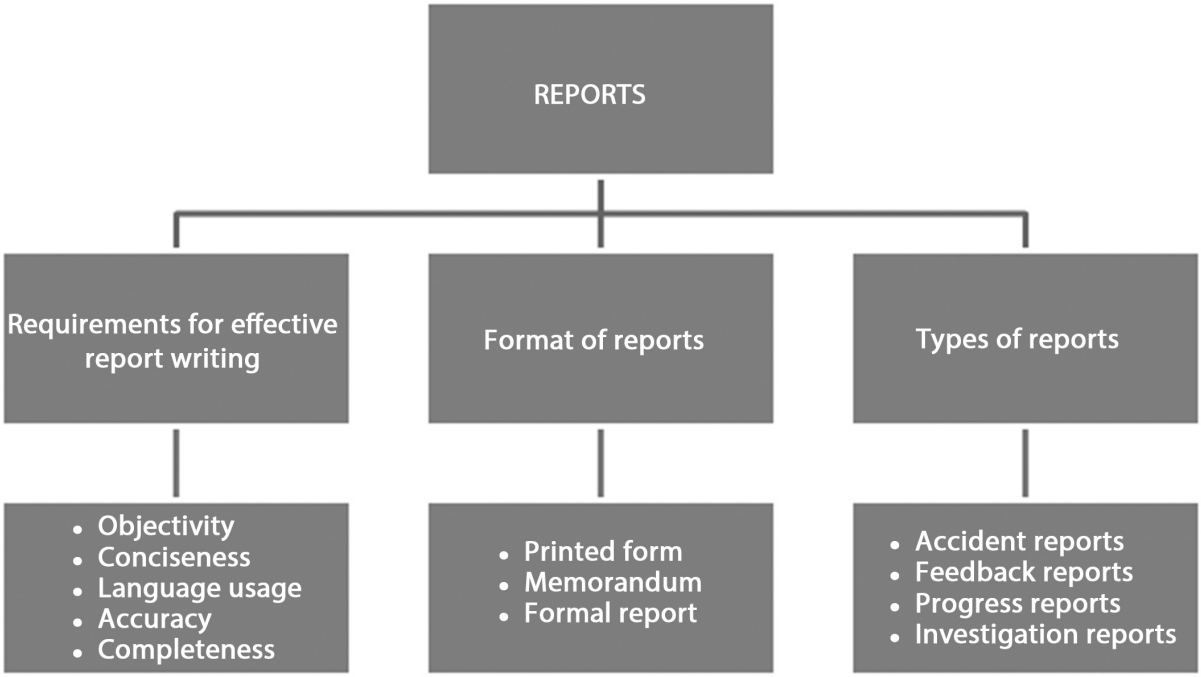
As far as the forensic investigator is concerned, the main function of a report is

- to inform either the client or the manager of progress, findings or the result of an investigation;
- to make a recommendation; or
- to request further instructions.

Apart from prescribed reporting intervals, it is always a good idea to keep management informed about developments in an investigation because it keeps them aware of what is happening, which is important. Keep in mind that certain decisions have to be made on the basis of a matter that you must report on.

The following figure by Van Rooyen (2004:58) illustrates the reporting process.

FIGURE 5.1 : The reporting process



5.6 REPORT WRITING

While there are many types of reports, they all have to comply with the requirements set out in figure 5.1 above. Let's now turn to the formal, memorandum-style of reporting. This is the informative report where the reporter explains the background leading up to the investigation, how the investigation was done, persons interviewed, findings and recommendations. You must also remember that managers do not have a lot of time to read through unnecessary information, so it is always a good idea to include an executive summary, which is essentially a condensed version of the report. Should the manager wish to know more about a finding that you made or the reason for a recommendation, he/she can refer to the original text.

Let's now examine the structure of the report.

As has been mentioned above, the report is a formal, structured presentation that has been divided into specific, numbered paragraphs, each with its own heading. In paragraph 6.10 below, you will find a diagram that sets out the requirements for a report, according to Combrink (1992).

5.6.1 The introduction and background

This is the first paragraph. It is a description of the situation that you have been requested to investigate. It sets out the nature of the matter and gives as much information as possible on the reasons for your involvement. It sets out the scope of your mandate and the person from whom you received that mandate. If there are any timelines involved, they should also be mentioned here.

5.6.2 The purpose

This is the second paragraph and describes what your mandate is in more detail so that the person to whom it is addressed is able to verify that you have understood your mandate correctly and that you have made recommendations in line with the mandate.

5.6.3 The investigation

Paragraph three describes in detail how the investigation was conducted; the tactics and techniques used; and the problems encountered and how they were solved. It gives the names of persons interviewed and indicates whether or not they made statements.

5.6.4 Findings

This paragraph describes the findings of the investigation: It describes the reason for the problem in the first instance and then gives the result of the investigation. If any persons are involved in irregularities, it sets out the reasons why these actions are considered irregularities and the results of these actions, as well as any financial loss incurred.

5.6.5 Comments

Paragraph five is where the reporter gives factual comments on the situation and what the various options are to resolve the matter. It explores the options and comments on the financial and other human resource implications. It sets out the advantages and the disadvantages of each of the possibilities.

5.6.6 Recommendations

In this paragraph, the reporter makes recommendations based on the findings and the comments. Here the recommended option is set out, along with the reason why this option has been chosen. If necessary, it substantiates why a less advantageous option is recommended. It also recommends the name of the official responsible for the implementation of the recommendation/ s, should it/they be accepted, and sets out the time frame for implementation. If an implementation plan is called for, this would have been included in the comments.

5.6.7 Conclusion

This is the final paragraph and it extends thanks to those persons who assisted the person compiling the report. The cost of the investigation is mentioned here and the executive summary, which will be included on the first page of the report, is briefly referred to. All annexures to the report are also listed here, together with any reference works that may have been consulted. The reporter should then sign the report.

5.6.8 Approval

Below the signature of the reporter there should be sufficient space for the decision- maker to note any comments, as well as his/her final decision.

5.6.9 Executive summary

The executive summary is no more than one-and-a-half to two pages in length. It is a condensed version of the report, but it retains all the essential information.

The purpose of an executive summary is to inform the chief executive officer or other senior decision-maker, as briefly as possible, what the problem was, what actions were taken, what the results were, what possible solutions there are and why a particular solution is recommended. This summary contains the same paragraph headings as the report itself and refers, by means of paragraph numbers, to important issues in the main report that must be brought to the reader's attention.

5.6.10 Example of the structure of a report

Below is an example of the structure of a report, as suggested by Combrink (1992).

FIGURE 5.2 : A diagram setting out the structure and form of a report

COVER PAGE

- Name of organisation requesting the report
- Reference number
- Subject of the instruction

INDEX

- Capital letters
- Underline headings
- Number paragraphs
- Number the pages

DEFINITIONS, ANNEXURES AND ATTACHMENTS

- New page – marked numerically
- Annexures are marked alphabetically and are not vital to the report.
- Attachments are numbered numerically and are vital to the report.

ADDRESSEE

- Person to whom the report is addressed

TITLE

- Subject of the report

INTRODUCTION

(PART ONE)

- Same page as title and deals with the following:
    1. Instruction, date given, date received, nature of instruction and reference number
    2. Purpose and reason for the investigation
    3. Background to the matter
    4. Planning and methods – interviews held, questionnaires, inspections and research

EXECUTIVE SUMMARY

(PART TWO)

1. Finding
2. Comments
3. Recommendations (refer to par 3.3 of main report)
4. Financial implications
5. Implementation

MAIN REPORT

1. Findings
2. Comments or conclusions
3. Recommendations

CONCLUSION

1. Acknowledgement and thanks
2. Certification – name of reporter and signatures

Source: Adapted from Combrink (1992)

ACTIVITY 5.1

Make a list of the various kinds of reports that you can think of and note the purpose of each.

5.7 RECORDING

When we refer to recording, there are a number of possibilities. In the forensic investigation process, recording refers to the way in which evidence is obtained and documented, the manner in which statements and findings are obtained, and the format in which this is done and then stored.

We speak of a witness statement being recorded in writing. When judicial proceedings are recorded, they have either been taken down in longhand or recorded on a device such as a tape recorder. Since the advent of video recording machines, investigators have used these to record the scene of a crime, interviews with witnesses or exhibits that are too large to bring to court.

We refer to the following collectively as "devices and apparatus that generate evidence":

- voice-recording devices, such as tape recorders, digital voice recorders, cassette voice recorders, reel-to-reel voice recorders, dictaphones, cellphones, telephone answering machines and others
- video cameras, which also record sound; cellphones with video capability; and old-fashioned movie cameras
- cellphones, which have become increasingly sophisticated with each new generation of devices
- computers with video capability, such as Skype
- cameras, which used to work with reel film, then with cassettes, and nowadays they take the form of digital cameras. In some cases, the latest cellphones contain digital cameras that are more powerful than the digital cameras of a few years ago. They are able to perform various tasks using Photoshop, which makes it possible to enhance, change and rework any digital photograph.

As technology develops on a daily basis, it becomes easier to manipulate digital devices. This means that whereas in the past you could not dispute a photograph showing the accused involved in committing a crime, these days, with all the enhancement and manipulation of digital devices that is possible, it is far easier to dispute the authenticity of images that were captured digitally. Therefore, you have to prove a number of things before a court will be prepared to accept the evidence captured on a digital device as proof. These requirements will be discussed in more detail below.

In general, there are great advantages to the use of photographic equipment in the field of investigation. Van Rooyen (2001:174) mentions the following advantages:

- to help the investigator recall the details of what he/she saw
- to explain what was seen to someone else, perhaps in court
- to enable the client, or the court, to examine the evidence instead of relying on the witnesses only.

While the admissibility of photographic evidence in court will be discussed a bit later, Van Rooyen (2001:174) warns that you should never discard or destroy spoiled or damaged negatives if you have used a film camera because someone may remember that you took more photographs, which you produced in evidence. This could result in your being accused of suppressing or tampering with evidence and could severely affect your credibility as well as your case. This is especially true when making use of a reel-to-reel tape-recording machine.

5.7.1 Video recordings

Video work is defined as any series of visual images (with or without sound) produced electronically by the use of information contained on any disc, magnetic tape or any other device capable of storing data electronically and shown as a moving picture.

Video recording is defined as any disc, magnetic tape or any other device capable of storing data electronically containing information by the use of which the whole or a part of a video work may be produced (http://www.tradingstandards.gov.uk).

A video recording is admissible as evidence in court, provided that you are able to present evidence of who made the recording and the date, time and place it was made. Before you make use of a video recording, you must ensure that the medium you are using to make the recording is clean or has not been used before. If the medium has been used before, you will have to explain to the court where the scene you are relying on as evidence in your case starts and ends, as well as why you have used a medium that has been used previously. To avoid this kind of inconvenience, it is preferable to use a new medium.

You will also have to be able to identify the persons or the images that appear on the recording. If you are unable to do this yourself, you will need a witness to do so for you. You will also have to prove that the medium you used to make the recording is genuine and that it has not been tampered with. You can be certain that the defence counsel will attack the admissibility of the medium if it proves to be damaging to the accused.

You should also bear in mind that the defence is entitled to view the recording, so it is always a good idea to have a working copy made, which can be placed at their disposal. They will undoubtedly also want to see the original to compare the two.

The original must be kept safe while in your possession. Remember that once it is handed in as an exhibit, it becomes part of the court record and is kept by the registrar or clerk of the court. It has happened in the past that after a matter was disposed of in court, the matter later went on appeal and the Supreme Court of Appeal wished to view the exhibit.

5.7.2 Photography

There are a number of definitions of "photography":

- "The science which relates to the action of light on sensitive bodies in the production of pictures, the fixation of images, and the like" (http://www.brainyqoute.com).
- "The art or process of producing images by the action of radiant energy and especially light on a sensitive surface (as film or a CCD chip)" (http://www.merriam-webster.com).
- "A device for recording an image of an object on a light-sensitive surface; it is essentially a light-tight box with an aperture to admit light focused onto a sensitized film or plate" (http://britannica.com/EBchecked/topic/90842/camera).

Photographs are admissible as evidence in court on the same basis and subject to the same rules that apply to videotapes. You must present evidence as to where, when, by whom and under what circumstances the photograph was taken. As in the case of the video operator, the photographer must give evidence that he/she took the photo; that it was a new, unused film; that he/she developed it; and that it could not have been accidentally mixed up with another film or photograph containing the damaging evidence. It may sound ridiculous to you to have to obtain this evidence, but experience has shown that the defence will try any angle to cast doubt on the validity of your evidence.

You must also be able to identify the persons in the photograph, which may prove to be difficult if the photograph was taken automatically, such as where a camera has been set up to take a photograph automatically if triggered by something. The admissibility of the photograph as evidence is not affected just because it was taken automatically; in such a case, the person who

set up the camera should be called to explain how it was set up and what triggered it to take a photo. Once the photograph is presented in court, you will have to be able to identify the person or the image to the court.

The easiest way in which to do this is by asking the accused/defendant whether it is him or her in the photograph. If they deny it, obtain this evidence from a friend or another person who knows them.

5.8 DIGITAL DEVICES

Digital devices refer to both cameras and recorders, which are used to store data messages.

5.8.1 Admissibility of data messages

Section 1 of the Electronic Communications and Transactions Act 25 of 2002 – which replaced the Computer Evidence Act 57 of 1983 – defines data as follows:

(i) Data is described as "electronic representations of information in any form".
(ii) A data message is described in section 1 as "data generated, sent, received or stored by electronic means and includes: –

- voice, where the voice is used in an automated transaction;
- a stored record".

The evidence generated by data devices has been found to be admissible as evidence in court in terms of the provisions of section 15 of the Electronic Communications and Transactions Act 25 of 2002, which provides as follows:

15 Admissibility and evidential weight of data messages

(1) In any legal proceedings, the rules of evidence must not be applied so as to deny the admissibility of a data message in evidence:
  (a) On the mere grounds that it is constituted by a data message; or
  (b) If it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

(2) Information in the form of a data message must be given due evidential weight.
(3) In assessing the evidential weight of a data message, regard must be had to:
  (a) the reliability of the manner in which the data message was generated, stored or communicated;
  (b) the reliability of the manner in which the integrity of the data message was maintained;
  (c) the manner in which its originator was identified; and
  (d) any other relevant factor.

(4) A data message made by a person in the ordinary course of business, or a copy or printout of or an extract from such a data message certified to be correct by an officer in the service of such person, is on its mere production in any civil, criminal, administrative or disciplinary proceedings under any law, the rules of a self-regulatory organization or any other law or the common law, admissible evidence against any person and rebuttable proof of the facts contained in such record, copy, printout or extract.

ACTIVITY 5.2

1. What is "best evidence"?
2. Where, in section 15 of the Electronic Communications and Transactions Act, does it mention "continuity of possession"?

3. Who do you think should give evidence as to the capturing of images on a digital device?

As far as the technical operation of these devices is concerned, an image taken by them is not stored onto a film, but in the camera's own memory or some storage device, such as a memory stick. To access the image, it is either played back by the device or it is printed or transferred to a disc to be viewed separately.

5.8.2 Digital recording

In terms of the provisions of the Electronic Communications and Transactions Act 25 of 2002, data is defined as "an electronic representation of information in any form". It defines a data message as "any data sent, received or stored by electronic means and includes both voice recordings as well as any stored record".

Source: Van Rooyen 2004:170

5.8.2.1 Cellphones

Most cellphones have digital cameras that are an integral part of the phone itself. Not only is this extremely handy, but they are available to most people who, in the past, may not have had access to such devices. If you just consider the cost of purchasing a brand-name digital camera as opposed to the cost of a digital camera that forms part of your cellphone, the latter is clearly the better option. The other advantage is that the image may be transmitted, within a few seconds of being captured, to anywhere in the world.

5.8.2.2 Digital photography

A digital camera is defined as "a device for making digital recordings of images" (http://www.britannica.com) and may, therefore, be classified as a digital device, as set out in paragraph 8 above.

There is no difference between a digital camera that forms part of a cellphone and an expensive state-of-the-art digital camera. They both produce images that are stored in the memory of the device, as set out in paragraph 8 above. Probably the only real difference is the quality of the image.

The greatest advantage of a digital camera is the fact that images can be reviewed immediately after they have been captured. This makes it possible to retake an image that is not clear. Once the image is satisfactory, it can be printed. The image can then be stored, retrieved or sent via the internet. When viewed on a computer, you can "zoom" in (enlarge parts of the image) and move around within the image to see something in the background, which may not have seemed important at the time the image was captured, but may become important later. Storage of the images is also easy because they take up very little space. Nevertheless, the great advantage of digital imagery could also prove to be a disadvantage, because the storage device can easily be stolen or damaged. Therefore, it is important to protect the storage device and keep it safe.

ACTIVITY 5.3

1. Do you know how to seize and secure digital evidence?
2. Do you know whom to contact to assist you in this regard?

5.9 LEGAL REQUIREMENTS

As far as the admissibility of both digital and film photographs are concerned, the provisions of section 232 of the Criminal Procedure Act 51 of 1977 provide as follows:

232 Article may be proved in evidence by means of photograph thereof

(1) Any court may in respect of any article other than a document, which any party to criminal proceedings may wish to produce to the court as admissible evidence at such proceedings, permit such party to produce as evidence, in lieu of such article, any photograph thereof, notwithstanding that such article is available and can be produced in evidence.

(2) The court may, notwithstanding the admission under subsection (1) of the photograph of any article, on good cause require the production of the article in question.

Many times it is impossible to produce the original article in court. Examples include graffiti sprayed onto a wall or something written on a surface that is too large to seize. In such cases, a photograph serves the purpose well. Especially in criminal cases, where a crime scene has been photographed and then stored, the photograph will serve as a permanent record, provided the requirements been complied with.

As far as digital devices are concerned, the requirements are very important. The requirements set out in sections (a), (b) and (c) of the Electronic Communications and Transactions Act, are self-explanatory and you should comply with them to prove that the images are those of the original that were taken, as well as by whom they were taken, how and where they were stored, and that no contamination or damage occurred.

5.10 SUMMARY AND CONCLUSION

Worldwide, investigators face problems relating to obtaining evidence to prove the guilt or innocence of a person. In this process, they have to use many techniques and tactics to provide the information they seek.

It is vitally important that investigators know not only the law and particular rules surrounding an investigation, but also how to report on their findings in such a way that the recipient is able to make an informed decision. The process of obtaining the information on which a report is based must be legal and transparent. This involves not only questioning and interrogation, but also the use of recording apparatus such as recorders and other devices that are able to capture and store images and voice recordings.

LIST OF REFERENCES

ACFE (Association of Certified Fraud Examiners). 2008. Managing the business risk of fraud: a practical guide. Available at: http://www. acfe. com/uploadedFiles/ACFE_Website/Content/documents/managing-business-risk.pdf (accessed 4 January 2010).

Clark, RV & Eck, J. 2004. *Become a problem-solving crime analyst.* London: Jill Dando Institute of Crime Science.

Combrink, J. 1992. *Hoe om 'n verslag te skryf*. Tafelberg: Goodwood.

Grogan, J. 2007. *Workplace law.* 9th edition. Cape Town: Juta.

Hiemstra, VG & Gonin, HL.1992. *Trilingual dictionary.* 3rd edition. Kenwyn: Juta.

Holtzhausen, N. 2007. Whistle blowing and whistle blowing protection in the South African public sector. DLitt et Phil thesis, University of South Africa: Pretoria.

http://en.wikipedia.org/wiki/Anton_Piller_order (accessed on 1 August 2010).

http://en.wikipedia.org/wiki/Emotional_intelligence(accessed on 12 March 2010).

http://en.wikipedia.org/wiki/Scientific_method (accessed on 12 March 2010).

https://en.wikipedia.org/wiki/Tactic (accessed on 12 March 2010).

http://en.wikipedia.org/wiki/Technique (accessed on 12 March 2010).

http://eqi.org/eidefs.htm (accessed on 12 March 2010).

http://www.acts.co.za/public_finman/schedule_3_other_public_entities.htm (accessed on 18 August 2009).

http://www.brainyquote.com/words/ph/photography202406.html (accessed on 8 August 2010).

http://www.britannica.com/EBchecked/topic/90842/camera (accessed on 8 August 2010).

http://www. capegetaway. gov. za/eng/yourgovernment/gsc/595/services/11455/17811 (accessed on 18 August 2009).

http://www.capegetaway.gov.za/eng/your_gov/595/public_entities/5801 (accessed on 18 August 2009).

http://www.merriam-webster.com/dictionary/photography (accessed on 8 August 2010).

http://www.thefreedictionary.com/tact (accessed on 12 March 2010).

http://www.tradingstandards.gov.uk (accessed on 8 August 2010).

http://www.wikipedia.org/wiki/Lateral_thinking (accessed on 26 April 2010).

http://www.wisegeek.com/what-is-abstract-thinking.html(accessed 26 April 2010).

Innes, M. 2003. *Investigating murder: the police response to criminal homicide*. Oxford: Oxford University Press.

Iyer, NK & Samociuk, M. 2006. *Fraud and corruption: prevention and detection.* Aldershot, UK: Gower.

Joubert, C (ed). 2001. *Applied law for police officials.* 2nd edition. Lansdowne: Juta.

Joubert, S. 2000. A criminologist on "whistle-blowing". *CRIMSA Newsletter* 24:10.

Kloppers, P. 1997. Behoort die whistle blower beskerm te word? *Stellenbosch Law Review* 8(2):237–248.

Knobel, JC (ed). 2006. *Law of delict.* 5th edition. Durban: Lexis Nexis Butterworths.

Marais, CW. 1992. *Physical evidence in crime investigation*. Pretoria: Henmar.

McLeod, T (ed). 1986. *Collins pocket English dictionary*. Glasgow: William Collins and Sons.

Miceli, MP & Near, JP. 1992. *Blowing the whistle: the organizational and legal implications for companies.* New York: Lexington Books.

Nickell, J & Fischer, JF. 1999. *Crime science. Methods of forensic detection*. Lexington: The University Press of Kentucky.

Public Service Commission. 2002. *Explanatory manual on the code of conduct for the public service. A practical guide to ethical dilemmas in the workplace.* Pretoria.

Robertson, JC. 1997. *Fraud examination for managers and auditors.* Austin, TX: Viesca Books.

Silverstone, H & Sheetz, M. 2004. *Forensic accounting and fraud investigation for non-experts*. Hoboken, NJ: John Wiley & Sons.

Smit, PJ & Cronje, GJ de J (eds). 2003. *Management principles. A contemporary edition for Africa*. 3rd edition. Lansdowne: Juta.

South Africa. Department of Justice and Constitutional Development. 2000. Protected Disclosures Act 26 of 2000. Pretoria: Government Printer.

Stalcup, K. 2010. How a simple misconception can trip up a fraudster and how a savvy CFE can spot it. *Fraud Magazine*, January/February.

Swanson, R, Chamelin, NC & Territo, L. 1977. *Crime investigation*. Santa Monica: Goodyear.

Swanson, CR, Chamelin, NC & Territo, L. 2003. *Criminal investigation*. 8th edition. Boston: McGraw-Hill.

Technikon SA. [Sa]. *Investigation of crime I: study guide for OVM 151RE*. Florida.

Tshaka, RS. 2010. Notes on ethics as a cornerstone for social cohesion. Paper presented during a seminar held at the Innovation Hub, Pretoria, 30 April.

Van der Westhuizen, J (ed). 1996. *Forensic criminalistics*.2nd edition. Johannesburg: Heinemann.

Van Rooyen, HJN. 2004. *Investigation – the A–Z guide*. Pretoria: Crime Solve.

Van Rooyen, HJN. 2007. *Crime scene investigation*. Pretoria: Henmar.

Van Rooyen, HJN. 2008. *The practitioner' s guide to forensic investigation in South Africa*. Pretoria: Henmar.

Zulawski, DE & Wicklander, DE. 2002. *Practical aspects of interview and interrogation*. 2nd edition. Washington, DC: CRC Press.

GLOSSARY

A

aberatio ictus	misdirection of the blow
ab initio	from the beginning
actio	claim/action
actio liberia in causa	the doctrine that the perpetrator of a deed who renders himself/herself criminally irresponsible in order to commit a crime while in that state is deemed to be fully responsible
actus	act/conduct
actus novus interveniens	an intermediate happening
actus reus	element of action in a crime
addendum	addition/assumption
ad hoc	for this special purpose
ad idem	of one mind/unanimous
ad infinitum	without limit/indefinitely
ad litem	for the purpose of the (pending) suit
ad rem	to the point
ad valorum	in proportion to the (estimated) value (of the goods)
a fortiori	all the more
alias	an assumed name
alibi	elsewhere (proof that the accused was elsewhere when the crime was committed)
aliunde	from another place or source
amicus curiae	friend of the court
animus intention/purpose	intention/purpose
animus furandi	intention of stealing/committing theft
animus possidendi	intention of possessing
a quo: the court *a quo*	whence/from which: the court from which an appeal is lodged
audi alteram partem	hear the other party/hear both sides
autopsy	post-mortem examination
autrefois acquit	previously acquitted
autrefois convict	previously convicted

B

bias	prejudiced
bona fide	in good faith/honest intention
boni mores	good morals
bonus paterfamilias	good family father/reasonable man

C

calumnia	false charge/malicious accusation
captis deminutio	curtailment of legal status (or capacity)
caveat	caution
caveat emptor	let the purchaser be on his/her guard/buyer beware
causa	cause
causa causans	decisive, determining cause
cessante ratione legis	if the justification (reason) for a law falls away, the law itself falls away too
cognoscitur a soclis	rule of interpretation which means that the meaning of a word is determined by others used with it
compos mentis	in one's right mind
consensus ad idem	agreement (to the same thing)
condicio sine qua non	indispensable/essential condition
condictio	an action for reclaiming something that has been obtained from the plaintiff without lawful cause or from a mistaken or immoral motive
contra bonos mores	against the good morals
contra fiscum	in case of ambiguity, the law is interpreted against the receiver of revenue
contrectatio	removal
corpus	thing
corpus delicti	the tangible object of the crime/exhibit
corruptisima republica plurimae leges	when the state was most corrupt, the laws were most numerous
crimen	crime
crimen iniuria	infringement of someone's right to dignity, honour and reputation
culpa negligence	negligence
culpa lata	gross negligence
curator ad litem	curator for the conduct of a suit
curia	in court/the bench
curia adversari vult	the court wishes to consider its verdict
curriculum vitae (CV)	career coverage/report

D

de facto	in fact/as a matter of fact
de jure	by law/legally
delegatus delegare non postest	a delegate cannot delegate
delictactionable	wrong
delirium tremensa	psychosis of chronic alcoholism involving tremors and hallucinations
de minimis non curat lex	the law does not concern itself with trifles
de novo	anew/afresh
derelicta	abandonment
detentio	holder
dictum (plural: *dicta*)	remark/saying
dignitas	dignity
diligens paterfamilias	reasonable man

doli incapax	unaccountable
dolus	intention
dolus directus	direct intention
dolus eventualis	legal intention
dolus indirectus	indirect intention

E

ebrius	a drunk person
eiusdem generis	rule of the same kind/sort (used in the interpretation of statutes)
emptor et venditor	purchaser and seller
en route	on the way
eo nomine	under that name
error	mistake/error
esprit de corps	a feeling of devotion to and pride in the group one belongs to
estoppel	the principle that precludes a person from asserting something contrary to what is implied by a previous action or statement of that person or by a previous pertinent judicial determination
exceptio	defence
exceptio doli	defence of fraud
ex facie	evidently; as would appear from the document
ex facie curiae	outside the face of the court/outside the court
ex hypothesi	in accordance with the hypothesis
ex mero motu	spontaneously/of his/her own free will
ex officio	by virtue of his/her office
ex parte	as the sole interested party/by (or from) one party only
ex post facto	arising from a subsequent event/with hindsight
expressio unius est exclusion	expression of one thing is the exclusion of the other
ex turpi causa non oritur actio	from a disgraceful cause no action arises
ex visceribus actus	from the bowels of a statute, i.e. a provision of a statute should not be construed on its own, but in the context of the entire act

F

facta probanda	facts to be proved/to establish the cause of action
felo de se	suicide
fisc/fiscus	treasury
fraus	fraud
functus officio	having discharged his/her office/no longer officiating
furtum	theft of the use of a thing

G

Generalia specialibas non degorant	general words (rules) do not derogate from special
genus	kind/make

H

habeas corpus	a writ requiring a person to be brought before a court or into court to investigate lawfulness of his/her restraint

I

imperativum	imperative/mandatory
impossibillium nulla obligation est	there is no obligation to do impossible things (to perform the impossible)
in absentia	in absence
in camera	in private/in chambers (the public being excluded)
in casu	in the case in question
in delictio	in violation of the law
inebriate	drunkard
in facie curiae	in the face of the court/in court
in favorem innocentiae	there is a presumption (in a case of doubt) that preference be given to innocence
in fine	at the end (of a book)
in flagrante delictio	caught red-handed/in the act
in forma pauperis	in the character of a pauper (may sue without liability or costs)
infra	hereunder
in fraudum legis	in fraud of the law/to evade the law
in limine	initial/at the very outset of the hearing
in loco parentis	in the place of the parent
in mora	in default
in pari delicto	equal wrong by both parties
in pari delicto potior est condition	in a case of equal wrong by both parties. the defendant is in the stronger position
in poenalibus causis benignius	in penal cases, the more favourable interpretation
interpretan dum est	should be adopted
in propria causa nemo iudex	no one can be the judge of his/her own case
in rem	real
in rem suam	concerning one's own affairs
inter alia	among other things
inter partes	between parties
inter vivos	between the living
in toto	wholly/completely
instrumentum noviter repertum	doctrine that the case already closed may be reopened on the ground that relevant but as yet unknown documents have come to light
intra vires	within the powers (or competence) of
ipsissima verba	the identical (the very) word
ipso facto	by the mere fact/by the very fact
ipso jure	by the law itself
iudicis est ius dicere non dare	it is the duty of a judge to expound/interpret the law, not to make it

iusta causa	just cause/lawful ground
iuris	jurist/legal expert
iustus error	pardonable error

L

lacuna	omission/gap/blank
lex	the law
lex non cogit impossibilia	the law does not compel the performance of impossibilities
lex non favet delicatorum	the law does not favour the fads (or wishes) of the dainty or fastidious
lex posterior derogate priori	a later statute (law) abrogates (repeals, takes away the effect of) a prior one
lis	dispute/action at law
litis contestatio	joining issue (in a suit/close of pleading in a civil case)
locus standi	right to be heard
locus standi in judicio	a right of appearance in court as a party/standing in court
lucidum intervallum	temporary sanity (of a disturbed mind)

M

mala fide	in bad faith
mandamus	court order ordering the commission of an act/an interdict in which a civil servant is concerned
maxima	the greatest/maximum
maxim	a general truth or rule of conduct expressed in a sentence
mens rea	guilty mind/criminal purpose of intention
mero motu	spontaneously/of his or her own accord
merx	article of trade
metus	fear
minor	underage; also used in a minority judgment
modus operandi	manner of operation
mora delay	
mutatis mutandis	after making the necessary changes

N

negotiorum gestio	spontaneous agent (without any mandate)
nemo debet bis vexari	no one ought to be harassed a second time for the same cause (crime)
nemo est suo delictio meliorum	no one can take advantage of his/her own wrong
nemo plus iurus ad alium transferre potest quam ipse haberet	no one can transfer more rights to another than he himself/she herself has
nexus	link/chain
nisi	unless
nolens volens	whether willing or not
nolle prosequi	refusal to prosecute
nomine officii	(NO)in his/her official capacity

non compus mentis	not of sound mind
non scripta	regard as unwritten
noscitur a sociis	the meaning of a word is inferred (known) from that of its companions (the accompanying words)
novus actus interveniens	a new cause intervening
noxious	hurtful/injurious/prejudicial
nulla bona	no goods (upon which to execute)
nulla poena sine culpa	no punishment without blameworthy state of mind (*mens rea*)

O

obiter dictum	a remark in passing
omissio	omission
omnia praesumuntur rite esse	all acts are presumed to have been lawfully done
acta donec probetur in contrarium	until proof to the contrary can be adduced
onus	burden of proof

P

pactum	agreement
pactum de non pretendo	agreement not to sue
particeps criminis	participant in a crime
pater est quem nuptiae	father is he whom the marriage points out
demonstrant paterfamilias	father (head) of the family/reasonable man
pauper	destitute/needy/poor
per capita	per head
per incuriam	through inadvertence/through an oversight
per se	by himself/herself/itself
pignus	pledge
plagium	manstealing/kidnapping
plus valet quod agitur quam	the real intention carries more weight than a
quod simulate concipitur	fraudulent formulation (or pretence)
postea	later
post-mortem	autopsy
pretium price/cost/value	
prima facie	at first sight/glance
prima inter pares	first among his/her peers
pro amico	for friendship sake/for a friend (referring to gratuitous services in court)
probandum	what is to be proved
probatio	proof
pro bono publico	for the good of the community
pro Deo	for God's sake – referring to the defence at state expense
pro forma	for the sake of form/as a matter of form
pro non scripta haberi	as never written/as though it had not been written
protocol	order of preference

proximate	nearest/next
proxy	mandate/full powers/full authority

Q

qua	as in the capacity of
quare	query/doubtful/problematical
quasi	pretend
quid pro quo	mutual consideration/something for something
qui facit per alium facit per se	he/she who acts through another (is considered) to act himself/herself
quis costodiet ipsos custodies?	Who guards the guards?
quod principi placuit, legis habet vigorem	the will of the emperor has the force of law

R

raptus	rape
ratio	reason/ground
ratio decidendi	ground for decision/court's ruling
re	in the matter of
res/rei	thing/object of rights
res aliena	thing of another
res communes omnium	things common to all
res corporalis	corporeal thing
res derelicta	abandoned thing
res fungibles	fungible things
res loquitor ipsa	it speaks for itself
res mentalis	mental reservation
res nullius	ownerless thing
respondeat venditor	the seller guarantees against latent defects
restitutio in integrum	return to the previous legal position
rex non potest peccare	the king can do no wrong
rixa	brawl/fight
rogare	ask/request

S

sciens non fraudutor	no one is knowingly the victim of deceit
semel mentitus semper menitur	once a liar always a liar
sensus non aetas invenit sapientiam	intelligence, not one's years lead to wisdom
seriatum	severally/individually/point for point
servamus et servimus	we protect and we serve
sic	odd but correct
socius	participant
socius criminis	accomplice
spes	hope/expectation
sponsalia	engagement to marry
stare decises	abide by/adhere to decided cases

sub judice	under consideration
sublata causa tollitur effectus	if the cause is eliminated, the effect ceases
subsecuta observatio	in the interpretation of laws, the established and customary construction put upon the law
subpoena	witness summons
sui generis	of its own kind/peculiar
supra	above

T

tenor	effect/import/tendency/trend
testis non iuratus nullam meretur fidem	an unsworn witness inspires no credence
tort	delict
toto	entirely
traditio	delivery
traditio brevi manu	delivery with the short hand
traditio longa manu	delivery with the long hand
trias politica	the division of the body politic so as to distinguish legislative, executive and judicial powers
trite	generally accepted (law)
turpis	disgraceful/infamous/mean
turpis causa	a base cause/immoral consideration
turpis persona	infamous/disgraceful person
turpitudo	infamy/vileness

U

uberrima fides	the most abundant good faith
ubi non est accusatory	where there is no accuser there is no judge
ibi non est iudexultra vires	beyond the scope of one's powers
uno principo illicto dato	if a single illegality is admitted, several others
plura sequuntur	follow
usus	use/precarious enjoyment of land
uxor	wife/spouse
uxor sequitur domicillium viri	a wife follows the domicile of her husband

V

verba ipsissima	the exact/the very words
verbatim	word for word
verbis	words
versari in re illicit	the doctrine that where one is engaged (or busy with) illegal activities, a second or further act from such illegal activities are per se also illegal
versus	against
vicarius non habet vicarium	a substitute (proxy) has no substitute (proxy)
vice versa	the other way round/conversely
vis divina	divine (or superhuman) force/act of God
vis major	irresistible force/act of God
viva voce	orally

voetstoots	without warranty/as it stands
volenti non fit iniuria	he/she who consents cannot receive an injury
voluntas coacta voluntas est	an expression of will uttered under coercion is still an expression of will