# CONTENTS

1. SPEAKERS’ PROFILE 3
2. INTRODUCTION 4
3. DEFINITION OF KEY CONCEPTS 5
4. CORPORATE GOVERNANCE 6
5. UNDERSTANDING GOVERNANCE PRINCIPLES 7
6. STAKEHOLDER RELATIONSHIPS 10
7. ETHICS CONCEPTS AND DISTINCTIONS 14
8. IMPORTANCE OF ETHICS 19
9. ETHICS OF GOVERNANCE 20
10. CODES OF ETHICS 21
11. ETHICS AND DECISION MAKING PROCESS 25
12. APPLYING THE DECISION MAKING PROCESS TO CASE STUDIES 27
13. RISK AND RISK MANAGEMENT 29
14. THE RISK MANAGEMENT PROCESS 32
15. KING III AND THE RISK MANAGEMENT PROCESS 40
16. INFORMATION TECHNOLOGY RISK 46
17. COMPLIANCE RISK 51
18. FRAUD 53
19. FACES OF FRAUD AND CORRUPTION 61
20. REDUCING FRAUD RISK 66
21. DETECTION OF FRAUD AND FRAUD AWARENESS PROGRAMMES 68
1. **SPEAKERS’ PROFILE**

**Olasesi Martins** is an expert trainer on Corporate Governance, Ethics and Risk. She is a skilled facilitator and presenter on leadership issues, ethics, risk and corporate governance for the last 17 years. Olasesi Martins is an attorney by profession, and holds a Masters Degree in Corporate Law and Governance. She is a trainer or workshop facilitator for company secretaries, governance officers and company administrators. She is a Fellow of the Chartered Secretaries Southern Africa (CCSA). She is a member of the Panel of Speakers for CCSA CPD Workshops. CCSA coverage is across South African, Zimbabwe, Singapore, China, Australia, Malaysia, and Canada. She is also an Associate Member of the Association of Arbitrators of Southern Africa. She is a Certified Ethics Officer with EthicSA and she is trainer on ethical matters. In addition; she is a seasoned speaker in international corporate governance / company secretarial conferences.

**Brian Smith** is an internal auditor by profession. He holds Post Graduate Certifications in Internal Auditing (C.I.A), Computer Auditing (C.I.S.A) and Fraud Investigation (C.F.E.). Brian has 36 years’ experience in Risk Management, Internal Auditing, Compliance, Corporate Governance, Ethics and IT Auditing and has also been responsible for Training of his staff and for presentations to General Management on all these topics. Brian has been responsible for developing an integrated Risk and Internal Audit Methodology that has been used, for the past 14 years, in one of the biggest services groups on the JSE, which operates in nine countries in Southern Africa, the United Kingdom, Europe and the Asia Pacific Region. Brian is a versatile trainer for executives, managers and administrators.
2. INTRODUCTION

This handbook is a detailed guide to the subject of corporate governance, ethics, risk and fraud. These are topical subjects at the heart of governance debates all over the world. This document highlights many of the key issues surrounding the concept of corporate governance, ethics, risk and fraud as they apply to all businesses in all sectors of the economy.

This document will provide the reader with all the relevant information that s/he needs to know on what corporate governance means and how to make your business a corporate citizen. Individuals are expected to behave in an ethical manner; however, ethics is a lot broader than that; ethical considerations are at the root of many problems which companies are dealing with. This document on ethics emphasises the need for improved awareness and focus on ethical matters.

Every business faces risks; the nature and severity of such risks may vary from one company to the other. Whilst some risks become insignificant with time, new risks emerge because risk is dynamic in nature; it changes with time. This document will assist the reader to understand the concept of risk as it applies to everyone either as an entrepreneur, a manager or as a layman on the street. It is important to know how to identify and evaluate risks to which a business is exposed in order to put appropriate measures in place to do any or a combination of the following; accept, avoid, mitigate, control or eliminate the risks. Risks could be positive in nature where there is a possibility that actual events might turn out positively than anticipated, businesses need to know how to take advantage of that too.

‘Fraud and deceit abound now more than ever before’ – Sir Edward Cole in 1602. As that statement may hold true today as it was in 1602, we have also realised that with time, virtues may be learned, such that core values such as honesty, diligence, responsibility, accountability and fairness become second nature to us as people. However, whilst we are being schooled in the art of becoming better people; businesses still need to deal with the issue of fraud in every aspect of economic activities. This guide will assist the reader to identify fraud risks in the business environment and how to deal with them decisively.
3. DEFINITION OF KEY CONCEPTS

3.1 DEFINITION OF CORPORATE GOVERNANCE, ETHICS, RISK AND FRAUD

- Governance is a system of controlling and directing an entity.

- Ethics is a set of principles of right conduct or a system of moral principles.

- Risk is the effect of uncertainty on objectives.

- Fraud is a deception deliberately practiced to secure an unlawful or undue gain.
4. CORPORATE GOVERNANCE

4.1 WHAT IS CORPORATE GOVERNANCE?

‘Corporate Governance is a system by which a company is directed and controlled’ – Sir Adrian Cadbury

It is true that the focus on corporate governance has been on the commercial sector and the public sector, especially in the large public companies where the separation of ownership from management is of a wider scope than for small companies, however, we must be mindful of the fact that corporate governance is also important for the voluntary sector. Many of the issues are the same, issues such as accountability; stakeholder relations, openness and transparency are relevant in all sectors. In recent times, research has shown that even performance evaluation is not only targeted at the public sector, even voluntary organisations are beginning to look at the possibility of measuring their performances.

Corporate governance is about the manner in which the affairs of company are managed towards the principal objective of meeting the reasons for its existence. For instance, it is about how powers are shared and exercised by the different stakeholders to ensure that company objectives are achieved.
5. UNDERSTANDING GOVERNANCE PRINCIPLES

5.1 UNDERSTANDING CORPORATE GOVERNANCE ISSUES

Corporate governance deals with the following issues which impact directly on sustainable business strategies:

a. **Rights and equitable treatment of shareholders** - Organisations should respect the rights of shareholders and help shareholders to exercise those rights. They can help shareholders exercise their rights by openly and effectively communicating information and by encouraging shareholders to participate in general meetings.

b. **Interests of other stakeholders** - Organisations should recognise that they have legal, contractual, social, and market driven obligations to other stakeholders which include employees, investors, creditors, suppliers, local communities, customers, and policy makers.

c. **Role and responsibilities of the Board of Directors** - The Board needs requisite relevant skills and understanding to review and challenge management performance. It also needs adequate size and appropriate levels of independence and commitment.

d. **Integrity and ethical behaviour** - Integrity should be a fundamental requirement in choosing corporate officers and board members. Organisations should develop a code of conduct for their directors, executives and other employees to promote ethical and responsible decision making.

e. **Disclosure and transparency** - Organisations should clarify and make publicly known the roles and responsibilities of board and management to provide stakeholders with a level of accountability. They should also implement procedures to independently verify and safeguard the integrity of the company's financial reporting. Disclosure of material matters concerning the organisation should be timely and balanced to ensure that all investors have access to clear, factual information.

5.2 THE NEED FOR CORPORATE GOVERNANCE

Corporate governance is important for all organisations; it creates transparency, strengthens confidence in management, and it is a form of protection for shareholders. Good corporate governance encourages the growth and sustainability of a business. Some of the challenges of a
small business include lack of managerial skills, lack of future business projection, absence of good governance structures, insufficient capital, uncontrolled drawings etc. Implementing corporate governance will reduce or eliminate some of these challenges facing small businesses.

5.3 CORPORATE GOVERNANCE PRINCIPLES

The key principles of corporate governance include core values such as accountability, responsibility, honesty, integrity, openness and transparency, mutual respect, performance evaluation and commitment to the company/organisation.

5.4 King III – SCOPE AND APPLICATION

King III applies to all entities regardless of the manner and form of incorporation. It is based on the principle: ‘apply or explain’. The King III Report is not legislative in nature, which means that it is not law but it may have an effect on the possible liability of directors if it is not complied with. For instance, non-compliance with King III may result in directors being held liable for not complying with the duty of care and skill. The Code does not address the application of its principles and it gives room for each entity to consider and decide which approach will best suit its size and complexity. However, the application of the Code may be mandated by law such as the JSE Listing Requirements.

The ‘apply or explain’ approach simply means for example that where the Board of directors takes a decision that to follow a recommendation from the Code will not be in the best interest of the company; that such a Board may apply another practice or apply the recommendation differently, provided that the practice being adopted will still achieve the objective of the overarching principles of corporate governance. In addition, the Board will also have to explain the need for such a deviation; detailing how the principles and recommendations were applied and the results. Where this procedure is followed, the company will be deemed to be compliant.

King III has extended the scope of corporate governance to a large extent with emphasis being placed on effective leadership, sustainability, and corporate citizenship. It requires the Board to act in the best interest of the company and to act as the custodian of corporate governance. It requires the Board to focus on the following:

1) Ethical Leadership and Corporate Citizenship
2) Board and Directors – Acting as focal point for and custodian of corporate governance
3) Effective and Independent Audit Committees
4) Governance of Risk
5) Governance of Information Technology
6) Compliance with laws, rules, codes and standards
7) Effective Risk Based Internal Audit
8) Governing stakeholder relationships
9) Integrated Reporting and Disclosure
6. STAKEHOLDER RELATIONSHIPS

6.1 STAKEHOLDER RELATIONS AND RELATED MATTERS

Effective management of relationships with stakeholders is crucial to resolving issues facing organisations. By using their influence, stakeholders hold the key to the environment in which the organisation operates and the subsequent financial and operating performance of the organisation. Thus the effective management of stakeholder relations is growing as a key focus of organisational sustainability.

The importance of stakeholder management is to support an organisation in achieving its strategic objectives by interpreting and influencing both the external and internal environments and by creating positive relationships with stakeholders through the appropriate management of their expectations and agreed objectives. Stakeholder Management is a process and control that must be planned and guided.

A stakeholder is any person, group or organisation who can place a claim on an organisation's attention, resources or output, or is affected by that output. Stakeholders have a stake in the organisation, something at risk, and therefore something to gain or lose as a result of corporate activity. Expectations are established and agreed for the manner in which communications are managed between stakeholders - who receives communications, when, how and to what level of detail.

The aim of stakeholder relations management is to influence stakeholder attitudes, decisions, and actions for mutual benefit. A stakeholder / stakeholder group expects the company to behave in a certain way with regard to the stakeholder's/ group's interests. Most often, the balance of power among different stakeholder groups is a key issue for consideration in corporate governance, especially where there are conflicts of interest, the company must have a water-tight strategy to deal with conflicting interests amongst its stakeholders and it must ensure that each stakeholder group exercises its rights/ power appropriately in line with laid down rules or charter. A company has a number of different stakeholder groups which may include the following:

a. Shareholders
b. Board of directors
c. Management
d. Employees
e. Customers/ Clients
As the stakeholders are different, so are their interests different from one another. That is essentially what gives rise to conflict of interest; for example, one major concern of employees is higher salaries, but sometimes, the company may be unable to implement an increment in staff salaries unless it cuts back on the dividend payout to the shareholders. The shareholders on the other hand want as much dividend as available from the company’s reserves.

Another example is the common scenario where there are conflicts of interest between the executive directors and the shareholders. Being the custodian of valuable information about the business, the executive directors know what is going on in the business, and so it is possible for the directors to decide how much information the company releases to its stakeholders. In addition, shareholders do rely on the board of directors to manage the company competently, and the shareholders are able to monitor the performance of the company through the company’s annual reports and financial statements.

The reliance of the shareholders on the information provided by the directors is based on trust that the information contained in the reports is correct, on the assumption that the directors are honest. The shareholders also rely on the auditor’s affirmation that the published financial statements do reflect the true financial position of the company.

The Organisation of Economic Cooperation and Development (OECD) highlighted the conflicting interests of stakeholders and succinctly put it thus;

“What makes corporate governance necessary? Put simply, the interests of those who have effective control over a firm can differ from the interests of those who supply the firm with external finance. The problem commonly referred to as a principal-agent problem, grows out of the separation of ownership and control and of corporate outsiders and insiders. In the absence of the protections that good governance supplies, asymmetries of information and difficulties of monitoring results in capital providers who lack control over the corporation, finding it risky and costly to protect themselves from the opportunistic behaviour of managers and controlling shareholders.”

The conflict of interest between shareholders and the board of directors is a key issue in corporate governance, and most of the corporate governance codes of conduct are directed at reducing these potential conflicts and managing stakeholder expectation for mutual benefit. It is also about understanding the material impact that organisations have on stakeholders and responding appropriately to stakeholder needs and expectations.
Potential conflicts may arise in the following areas:

a. Financial Reporting and Auditing  
b. Directors’ Remuneration  
c. Board – Stakeholder Relations  
d. Corporate governance & Risk Management  
e. Communication framework

6.2 APPROACHES TO CORPORATE GOVERNANCE

There are different approaches to corporate governance. These can be divided into three:

a. The shareholder value approach  
b. The stakeholder/ pluralist approach  
c. The enlightened shareholder approach

a. The shareholder value approach  
This is a well known approach which supports the viewpoint that companies are in business primarily to maximise the wealth of their shareholders. Under this approach, successful businesses are viewed as those paying regular dividends to its stakeholders. However, it is important to note that corporate governance has grown beyond focusing on the interest of one group of stakeholders, but a more encompassing approach is in favour of looking at the interests of shareholders, employees, suppliers, customers and other groups with vested interests in the company.

b. The stakeholder/ pluralist approach  
From a stakeholder’s perspective; this approach is concerned with achieving a balance between different goals: economic; social, environmental, safety, health and others. This approach holds directors accountable for company resources. It focuses on a broader viewpoint of looking at the varied interests of stakeholder groups such as the shareholders, employees and their families, suppliers of raw materials, purchaser of the company’s finished products. From the view of OECD, it describes the stakeholder approach as;

“From a public policy perspective, corporate governance is about nurturing enterprise while ensuring accountability in the exercise of power and patronage by firms. The role of public policy is to provide firms with the incentives and discipline to minimize the divergence between private and social returns and to protect the interest of stakeholders.”
c. **The enlightened shareholder approach**  
This approach encourages directors of a company to pursue the interests of their shareholders in an enlightened, holistic manner. It emphasises the need for directors of a company to create and maintain productive relationships with the different stakeholder groups. The enlightened view focuses on the need for directors to look at the interest of shareholders and other stakeholders in the short and in the long run. A major criticism of this approach is that most shareholders, being institutional shareholders do not fit the profile of enlightened investors.

6.3 **THE BEST PRACTICE IN CORPORATE GOVERNANCE**

There is no 'one cap fits all' strategy to corporate governance. Circumstances of companies differ, and what is applicable in one may not necessarily work in another company. However; it is very important for companies to apply a corporate governance approach that is workable for them, bearing in mind that corporate governance is not a once-off activity but a long term corporate culture. An effective governance policy recognises a governance framework and an integrated reporting system.

a. **Corporate Governance Framework**
A corporate governance framework is a detailed governance, risk and compliance system which synchronises governance with risk and compliance. It addresses all the issues within an organisation relating to strategy, processes, technology and people.

b. **Integrated Sustainability Reporting**
In South Africa, the King III Code on Governance, released in September 2009, recommends that organisations produce an integrated report. As the King Code falls within the Johannesburg Stock Exchange (JSE) listing requirements, listed companies were required to produce an integrated report for their financial years starting on or after 1 March 2010 (the effective date of the King III Code). This requirement was implemented ahead of formal standards or guidelines for integrated reports. However, an Integrated Reporting Committee (IRC), chaired by Professor Mervyn King, and founded by: The Association for Savings and Investment SA (ASISA); Business Unity South Africa (BUSA); Institute of Directors SA (IoDSA); JSE Ltd; and The South African Institute of Chartered Accountants (SAICA), was established to issue guidelines on good practice for integrated reporting. A working group was also created to develop a framework for integrated reporting. The integrated sustainability report is expected to provide essential information about the organisation in respect of its economic, social and environmental preservation activities. All of those will stand as the organisation's triple-bottom line reporting.
7. ETHICS CONCEPTS AND DISTINCTIONS

7.1 WHAT IS ETHICS?

Ethics is a set of principles of right conduct or a system of moral principles. To get a better understanding of what ethics is; kindly look at a few statements below and make your choices based on your interpretation of what ethics is.

- I am an ethical person/ I am not an ethical person
- I work for an ethical organisation/ I do not work for an ethical organisation
- I live in an ethical country/ I do not live in an ethical country

Please underline your choices above and motivate your answers in the spaces provided below:

Conventionally, ethics professionals use three key concepts to define Ethics. It is seen as a form of a triangle; an interaction amongst the concepts of ‘good’, ‘myself’ and ‘others’.
Ethics concerns itself with what is good (or right) in my personal (myself) interaction with others. Behaviour can thus be considered to be ethical when it is not merely based on what is good for oneself, but also considers what is good for others. It is important that each of these three central concepts should be included in a definition of ethics. Where any of the three key concepts is missing, the definition for ethics will be lost.

7.2 WHAT IS BUSINESS ETHICS?

Business ethics can be defined as the principles, norms and standards that guide an organisation’s conduct of its activities, internal relations and interactions with external stakeholders. Business ethics deals with the identification of appropriate standards of corporate behaviour which takes into consideration the impact that business has on all stakeholders. It balances profitability with corporate ethical culture.

7.3 WHAT ARE VALUES?

Personal values

Personal values are your own convictions as a person about what is good, acceptable and desirable. Your values are your core values as an individual. Example of such values could be honesty, trust, integrity, diligence, dedication, commitment etc.

- Some of my personal values are the following:

Assuming that you enter into a retail shop to buy a few groceries for the week. You pay for the items at the till, and you leave the retail shop. However, as you are about to enter into your car at the parking lot, you checked the change the till attendant gave you, and you realise you have been given thirty rand (R30) more than you are entitled to. What will you do?

- Would you agree that your response to the situation above is a function of your personal values as an individual?
Why do people have different values?

---

**Values in Organisations**

An organisation is a juristic entity, and just as individuals do have personal values, so do organisations too. There are three different types of values which an organisation can have; strategic values, work values and ethical values.

Strategic values refer to the shared conviction of the organisation about its desired objectives. As such strategic values indicate the direction into which the organisation wishes to move. The strategic values of organisations can usually be found in their vision and mission statements. In order to move the organisation into the direction articulated in its strategic values, each member of the organisation needs to do their jobs in a specific manner.

Work values are the priorities that organisational members should adhere to in their jobs as employees. Typical job values are punctuality, innovation, quality, etc. For any organisation to function optimally, good relations and interactions between stakeholders are required.

Ethical values are organisational core values which employees in an organisation need to commit themselves to for effective inter-personal relationship amongst all organisational stakeholders. Typical ethical values are respect, transparency, fairness, etc. Adherence to ethical values ensure that stakeholders inside and outside the organisation get along well with one another.

Mention a few organisational values from your company and highlight the impact of those values on stakeholders’ relations in your company.
7.4 ETHICS AND LAW

There are obvious similarities between ethics and the law, but there are also significant differences. Both ethics and the law strive towards stipulating what is right in human interaction and society. The law does so through a public and political process and employs the power of the state to ensure that all abides by the stipulations of the law. Ethics emanates from personal values and is done from a sense of internal obligation to do what is right.

7.5 PERSONAL AND ORGANISATIONAL ETHICS

Unethical behaviour is often blamed upon individuals with a defective moral upbringing (bad apples). This leads to the erroneous belief that the only cure for current unethical conduct, lies in educating a new generation of morally sensitive individuals (good apples). Although it is not to be denied that individuals with a defective moral upbringing pose a serious threat to society, it is also a gross oversimplification to blame all instances of immoral behaviour on so-called bad apples.

The social settings or organisations that individuals work in can also have either a good or corrupting influence on their moral character. People with good moral character can turn to unethical behaviour if they find themselves in organisations where unethical conduct is the norm. Thus bad barrels can corrupt even good apples. The opposite is equally true. Dubious or bad apples can be restrained from unethical behaviour should they find themselves in organisations that do not tolerate unethical behaviour, but rewards ethical behaviour.

Do you (dis) agree with these statements? Why? Or why not?
1. Child labour may sometimes be justified.
2. If you could save a life by telling a lie, you should do so.
3. People who kill others for a cell phone should forfeit their moral right to life.
4. Smoking is not good.

7.6 PROFESSIONAL ETHICS AND VIRTUES

It is not only people and business organisations that adhere to ethics. Specific groups in society also adhere to ethical standards. A profession is a typical example of a group of people who adhere to a set of ethical standards. One of these distinguishing features is that professions adhere to a self-imposed set of ethical standards. The purpose of these ethical standards is to ensure that members of a profession act in accordance with the spirit and purpose of the profession as well as to the benefit of the clients and members of society whom they serve.
A virtue is a trait that intuitionally enables one to do what is right. Professional virtues are those character traits which members of a profession are expected to have, for example, virtues of an auditor are independence, integrity and objectivity.

Professions normally do not only promote a set of ethical values and standards, but also try to inculcate certain virtues in the individual members of the profession. Virtues can be developed over time. A man with a short temper whose anger flares up at the most insignificant incident, can deliberately try to change this kind of behaviour that leads to personal embarrassment and harm to others. Over time, he can restrain himself until he has gained control over his temper. Through his deliberate attempts, he can succeed in overcoming his fierce temper and develop the virtue of being even tempered. Virtues are thus learned forms of behaviour that become second nature to us.

It is part of professional training to have the virtues of the profession to which one aspires to become a member. In the case of the accounting profession, for example, there are number of important virtues that accountants should acquire. The most important virtues are independence, integrity and objectivity. There is a general belief within the profession that when accountants and auditors have cultivated these virtues, they will be well disposed to act with integrity and enhance their own reputation and that of their profession, while also serving the well-being of their clients and society.
8. IMPORTANCE OF ETHICS

8.1 WHY WE NEED ETHICS

The importance of ethics cannot be overemphasised; some of the benefits are as follows:

- Ethics is the cornerstone of corporate governance.
- Ethics ensures the sustainability of a business.
- Good corporate reputation is built on a solid foundation of ethical culture.
- A culture of trust must be built on a corporate framework of ethical principles which are transparency/openness, competence, integrity and benevolence.
- Ethics play a major role in the prevention of fraud. Fraud prevention becomes a shared responsibility among the members of the organisation.

8.2 ETHICS AND GOOD GOVERNANCE

There is a relational connection between ethics and governance. The connection is based on the four ethical principles on which corporate governance structure is based: These values are:

- **Fairness**
  The organisation must ensure that in their decisions and actions they give consideration to the interests of all stakeholders of the organisation.

- **Accountability**
  The organisation must explain their decisions and actions to stakeholders affected by the organisation and give account to those stakeholders who require the organisation to do so.

- **Responsibility**
  The organisation should assume responsibility for all actions of the organisation and be willing to take corrective actions to keep the organisation on its strategic path.

- **Transparency**
  The organisation should disclose information in a manner that enables stakeholders to make a meaningful analysis of the organisation’s actions.
9. ETHICS OF GOVERNANCE

9.1 ETHICS OF GOVERNANCE - EFFECTIVENESS

In the ethics of governance, it is important that all the stakeholders should be involved; otherwise, the whole process becomes exclusive of one stakeholder or the other. An organisation’s Board, within the spirit of an inclusive approach to corporate governance, has to ensure that it takes due care of the interests of all stakeholders. Besides defining the purpose of the organisation, it has to identify and communicate the organisation values to all stakeholders.

Good governance is not only based on ethical values, but an important part of corporate governance deals with governing the ethical performance of an organisation. Integrated sustainability reporting or triple bottom-line reporting, encourages organisations to not only manage and report on their financial performance, but to do the same with regard to their social and environmental performance.
10. CODES OF ETHICS

10.1 PROFESSIONAL CODES OF ETHICS

Many professional organisations have codes of ethics which is a strategic way to set ethical standards for their members. The following are some of the reputable professional bodies which have codes of ethics for their members:

- SAICA: The South African Institute of Chartered Accountants
- SAIPA: (The South African Institute of Professional Accountants). Note that SAIPA has adopted the IFAC (International Federation of Accountants) code of ethics
- FPI: The Financial Planning Institute of Southern Africa
- IMCSA: Institute of Management Consultants of South Africa

What are the benefits for a profession or an organisation to have a good code of ethics?

Some benefits of having a code of ethics are:

- It enhances economic performance
- It helps build an ethical culture
- Stakeholders know where they stand (the contents of the code set clear parameters of desirable or undesirable behaviour)
- It provides security and predictability for employees
- It can contribute to building the organisation’s reputation
- It creates customer and stakeholder loyalty
- It builds trust between you and your stakeholders (the “others”)

Code of ethics are characterised by six key elements:

1. Purpose – what do you want the code to do for your organisation?
2. Process – How to get the buy-in of all your stakeholders
3. Format – How do you need to design the code of ethics?
4. Content – What guidelines do you need to include?
5. Tone – Should it be forceful or directional?
6. Implementation – How practical will the code be for your organisation to be effective?

10.2 ETHICS AS A CORPORATE CULTURE

Once an organisation has decided on its ethics management strategy, it still has a long way to go to entrench a culture of ethics. The challenge then, for the key role players involved in ethics management, is to translate the ethics strategy into meaningful corporate culture. Formal ethical culture will include the following:

- **Communication**
  An organisation has to clearly communicate its ethics expectations to all stakeholders. Also, the code of ethics has to be understood and applied by every employee. In addition, the organisation needs to know what kind of ethical issues their employees are confronted with, what type of unethical behaviour occurs, and what the “good news” ethics stories are. Communication about ethics forms the backbone of implementing an ethics strategy. Specific interventions that can be used to ensure effective communication on ethics includes ethics awareness programmes, ethics talk, an ethics help-line, a reporting channel for unethical behaviour, and ethics newsletters.

Since many codes of ethics are value-based they do not provide specific guidelines to deal with ethics issues that confront employees on a daily basis. Even those codes that are rule-based cannot cover all eventualities. For example: if an aspirational code that relies on employees to use their own discretion, forbids bribery, can an employee accept a gift from a supplier? and, what is the difference between a gift of an organisation’s T-shirt and an all-expenses paid weekend away? The fact is, employees need guidelines to deal with lesser decisions as well as issues that have more serious ethical consequences. How do they know what to do?

Many organisations have ‘ethics help-lines’ to assist employees in code interpretation or when they are confronted with difficult ethical issues. A typical help-line is a facility that consists of an ‘office’, website or telephone line that can be used by employees seeking answers to their ethics queries while remaining anonymous. Having a help-line naturally also raises the ethics awareness in an organisation – if the help-line receives many calls it does not necessarily mean that unethical behaviour is rife – it does, however, indicate that people think about ethics and are not afraid to ask questions about it.

Not all ethical issues can be adequately addressed by the ethics help-line. Complicated or serious issues require something in addition to the helpline. Some organisations therefore have a separate, anonymous facility or reporting line where unethical behaviour can be specifically reported. This also referred to as a whistle-blowing line. Although many organisations have an
internal reporting line to cater for ‘whistleblowers’, others opt for outsourcing it to external organisations that specialise in providing such services. The latter approach increases the chances that the person who reports unethical behaviour remains anonymous and thus not fall victim to potential victimisation.

- **Recruitment**
  If an organisation wishes to build a new ethics culture or maintain an existing one, it has to ensure that it attracts potential employees of integrity. When devising recruitment strategies the organisation has to put the word in no uncertain terms that it wishes to attract people that can align their ethical orientations with those espoused by the organisation. This approach to recruitment also builds the organisation’s reputation and enables it to attract talent. It also contributes to the creation of employees’ ethics awareness from the onset.

- **Selection**
  Many organisations opt for including integrity as a criterion for the selection of new employees or when promoting existing employees to positions that require ethical accountability. Given the assumption that integrity may indeed be measurable in a quantitative or qualitative manner, it may be included as a dimension to be assessed in a number of selection methods, e.g. interviews, reference checking, psychometric testing and assessment centre technology.

- **Orientation of new employees**
  Employees entering an organisation are susceptible to adopting the new organisation’s culture. If this culture is characterised by a strong ethics dimension, the new employees become aware of the organisation’s expectations regarding ethical behaviour from the very beginning. This is also the time to explain the code of ethics and how to apply its rules and guidelines.

- **Performance management and reward**
  An employee’s performance appraisal is usually based on a number of key performance areas that constitute a job. Employees are appraised on the extent to which they accomplish the demands defined by these key performance areas. Since ethics is not only the collective responsibility of all employees, but also the responsibility of each employee in his/her individual capacity, it should be “made real” for every employee – i.e. by making it an integral part of every job. This can be done by making it a stand-alone key performance area for some jobs that require continuous ethical decision-making, or at the very least, to integrate ethics into one or more key performance areas. In this way employees know what ethical performance is required and the extent to which it will be measured as part of a broader appraisal process. When employees are rewarded for their performance across several key performance areas, which include ethical performance as an independent key performance area, they are then, by implication, also
rewarded for their ethical performance. In this way employees are actually rewarded for ethical behaviour.

- **Training**
  A key focus area of organisational ethics training interventions is the training of employees to understand, interpret and apply the code of ethics. Such training is usually conducted by means of generic case studies as well as organisation specific ones. Employees should also be trained on their responsibilities in creating an ethical culture. Training on the purpose and use of helplines, as well as confidential reporting lines, are further components of ethics training.

- **Disciplinary procedures**
  Organisations react to unethical behaviour by dealing with transgressions, especially serious ones, in a swift and decisive way. Disciplinary structures and procedures are usually sufficiently informed and well-positioned to also deal with ethical transgressions.
11. ETHICS AND DECISION MAKING PROCESS

11.1 ETHICAL ISSUES

We often face situations where we need to make decisions that have ethical implications. Whenever our decisions affect what is either good or bad for ourselves or for others, we are dealing with ethical decisions. Like all other decisions that we make, our ethical decisions can be either excellent or poor.

In dealing with ethical issues, sometimes, Codes of ethics may not always provide all the answers; however, they provide necessary but not sufficient tools to assist with an ethical decision-making process. Ethics is bigger than the law in term of its scope. It is impossible for legislators, organisations and professions to anticipate everything that could possibly go wrong and to then make a law or rule to prevent the undesired behaviour. Professional practitioners therefore require ethical decision-making skills that could assist them in analysing ethical problems and in making calculated ethical decisions.

11.2 THE ETHICAL DECISION MAKING PROCESS

A wide variety of ethical decision-making tools exist. All these decision-making tools have the objective of structuring a thinking process that will result in sound ethical decisions. We will only discuss one of such decision-making tools. The decision-making process that is presented for the purpose of this module is structured according to the following questions:

- What alternatives are available for my consideration?
- Are the alternatives legal?
- Do the alternatives meet with professional/organisational ethical standards?
- Will I be able to disclose my actions?
11.3 DECISION MAKING TOOL

What alternatives are available for my consideration?

If Yes  Are they legal?  If No, Stop!

Do they meet with professional/organisational ethical standards?

If Yes  If No, Stop!

Will I be able to disclose my actions?

If Yes  If No, Stop!

Ethical Decision
12. APPLYING THE DECISION MAKING PROCESS TO CASE STUDIES

Case 1
At a function organised by your company in your company premises, shortly before the end of the function, you notice that your manager is busying putting cartons of drinks into the boot of his car. In that split of a second; he glances at you, smiles and says; ‘what the company doesn’t know wouldn’t hurt the company; erase this from your memory’. Then your supervisor says his goodbyes to everyone including you, and he drives out of the premises.
What do you do?

Case 2
A supplier overhears a conversation amongst your colleagues that today is your birthday; she quickly goes out to the shopping mall next to your office building to buy you a card and a box of chocolate. She comes back to your office, meets you at the reception, and wishes you ‘a happy birthday’ and gives you the birthday card and the box of chocolate.
What do you do?

Case 3
A supplier overhears a conversation amongst your colleagues that today is your birthday; she quickly goes out to the shopping mall next to your office building to buy you a card and a box of chocolate. She comes back to your office, meets you at the reception, and wishes you ‘a happy birthday’ and gives you the birthday card and the box of chocolate. The supplier is one of the three bidders your department is considering for a current tender.
What do you do?

Case 4
One of the accountants in your department has resigned and needs to be replaced. Your manager tells you that he wants to appoint Tyler, an accountant with one of your suppliers. He tells you to nevertheless go through the motions of following procedure by advertising the post internally. You agree that Tyler has the requisite qualification for the post. Once the applications have all been received, you realize that several more competent candidates from your subsidiary companies have applied. Your manager is however adamant that Tyler should be appointed.
What do you do?
Case 5
You get a call from a recruitment company requesting a reference for a person who is your acquaintance. This person was introduced to you a week ago by a mutual friend. You cannot claim to know her so well. What do you tell the caller?
13. RISK AND RISK MANAGEMENT

13.1 DEFINITION OF RISK MANAGEMENT

Risk is defined as “the effect of uncertainty on objectives” - ISO 31000.

Thus to be able to understand the risks that we face, we first need to understand our business objectives. The starting point is usually the establishment of the Vision and the Mission for the business venture. From this we define the business processes that will be needed to achieve this Vision and Mission and then we document the objectives for each of these business processes and finally identify the Risks.

For the purposes of this presentation, Risk Management is defined as “the process of Identifying, Analysing and Ranking the importance of the identified Risks with a view to Avoiding, Eliminating, Accepting or Reducing the Business’s exposure to Risk that could negatively affect the Start-up, Management or Growth of a business”.

An alternative definition of Risk Management is “the identification, assessment, and prioritization of risks, whether positive or negative, followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities”. (Wikipedia)

13.2 UNDERSTANDING RISK

Risk is a part of our lives and always has been. The minute we are born we face risk at every turn but accept this as part of living. Similarly when we start a business we face risk at every turn and simply accept this as the way it is. All that changed in 1994, with the publishing of the King Report on Corporate Governance, because Risk and Risk Management became business ‘buzz words’, and the process became something formal instead of something that we simply do without thinking about it.

Is Risk Management something new that we have to learn? Risk management is something that we have been doing every day, hundreds of times a day, without even thinking about it. For example, consider the risk management function that you undertake when you get dressed in the morning:

- **The Objective** To go out of the house but still remain dry and warm.
- **The Risk** Getting Cold or Raining Wet.
The Business Risk Management process is made up of various steps that build upon each other. These steps are:

- **The Control**
  Putting on a long sleeve shirt, long pants, socks and shoes and taking along a waterproof jacket

- **The Company Vision**
  Where we wish the business to go.

- **The Mission**
  What we want the business to achieve at a macro level.

- **Business Processes**
  To achieve the Vision and the Mission, the business will have to perform various business functions (processes) e.g. Purchasing, Stock Logistics, Sales, etc.

- **Objectives**
  To enable management to determine what the Risk is – the effect of uncertainty on objectives – we need to understand what it is we are trying to achieve from each business process.

- **Risks**
  The risk is simply the event that will prevent us from achieving our objectives. We must remember that risk is not always a negative (something that occurs to prevent us from achieving the objective), but could also be not recognising an opportunity that would help us to achieve the objective.

### 13.3 AN EXAMPLE OF A RISK UNIVERSE

Most companies would need to identify the business processes that are needed to achieve their Vision and Mission from scratch, and this is very time consuming. So to assist in this process, we have developed a Risk universe that identifies the business processes that we feel a standard (stock based) business would require.

This Chart reflects

- 5 Categories of Risk, being
  - Social & Ethics,
  - Financial Risk,
  - Operational Risk,
  - Information Technology (IT) Risk, and
  - Compliance Risk.

- 16 Business Areas.

- 65 Business Processes, excluding Business Specific Processes e.g. Manufacturing, which would need to be added if there are processes not mentioned in the chart.
Within these 65 business processes, there exists numerous Risks (347 identified in the Risk and Control Framework based on this model) and under each risk a host of controls (in excess of 18 000 controls to select from based on the business management style and methods).

Fig 4.1
14. THE RISK MANAGEMENT PROCESS

14.1 BUSINESS PROCESS SELECTION

The Business Process Selection is the first step in the Risk Management Process and for this we consider an extract from our definition – viz. The process of identifying risk

The Risk Universe has listed 65 business processes, but not all of these would necessarily be applicable to your business, so you would need to select those that are applicable and consider only those specifically for your business.

For example:
- If your business does not sell on credit, you could eliminate the Debtors Business Process, or
- If your business only buys for cash, you could eliminate the Creditors Business Process.

14.2 RISK ANALYSIS

The second step in the Risk Management Process is Risk Analysis and for this we consider an extract from Definition – viz. The process of c. analysing and ranking the importance of the identified risks

Once you have identified the business processes that are applicable to your business, and you have defined the objectives of each of these business processes, and have identified the risks that could prevent you from achieving these objectives, you need to analyse the risk and rank these according to:
- The Likelihood that the risk will occur, and
- The Impact that the risk will have if it does occur

An example of how a risk analysis could be used is depicted in Figure 5.1 below, which shows the Risk of Impact on the International Space station by micrometeorites and space debris.
The more traditional manner in which to depict the risk analysis is in a Risk Matrix, where the Impact is depicted on one axis and the Likelihood on the other axis. In this type of scatter graph each risk is mapped according to the Impact and the Likelihood as rated by management during the risk assessment and the risk rating is drawn from the shading on the graph, according to the block in which it falls. (see Figure 5.2 below).

Thus if the impact of a specific risk was rated as 2 and the likelihood was also rated as 2, the risk rating would be in block 6 and thus a Low Risk. Likewise if the impact was rated as 4 and the likelihood rated as a 3, the risk rating would fall into Block 18 and would thus be rated as Medium Risk. Similarly if the impact was rated as 5 and the likelihood rated as a 5, the risk rating would fall into Block 25 and would thus be rated as High Risk.

Traditionally the risk rating is on a scale of 3 with High, Medium or Low as the ratings, but some practitioners add an additional category of extreme or some similar name for blocks 23 to 25. However, it is submitted that, this adds an unnecessary level of complexity, as the reaction to a high risk and an extreme risk should be similar as both should trigger alarm at Board level and require immediate reaction. Also some risk practitioners use a scale of 1 to 10, which may lead to a lot of discussion on each point which is not beneficial to the risk analysis process.
Management would be required to rate the Impact and Likelihood of each risk but to achieve this on a uniform basis each manager would need to use similar criteria when performing the rating or this would lead to different ratings of similar risks by one manager or conflict between managers when comparing ratings. The manner in which this can be achieved is to set up a table (see Figure 5.3 and Figure 5.4 below) which gives the criteria used to allocate a risk score of 1 to 5.

The correct name given to these tables is ‘the Risk Appetite’ this should be set or authorised by the Board.

14.3 RISK IMPACT

It is not always possible to quantify the impact of a given risk in monetary terms and thus it is recommended that the Board should agree on the various criteria for assessing the risk impact. The example given below gives 3 additional criteria, but these could be added to or reduced depending on the complexity of the business being analysed.

The criteria below have been used by one of the largest group of companies listed on the JSE and proved adequate.

The level of impact used for each of the risk levels would vary from one business to another - e.g. a business with an annual turnover of R5 mil would have much lower monetary value for the 5 risk
levels than the example. Similarly, ‘severe’ system unavailability in a bank would probably be closer to 30 minutes to an hour.

<table>
<thead>
<tr>
<th>Level</th>
<th>Non-Financial Impact Description</th>
<th>Quantitative</th>
<th>Reputation</th>
<th>Systems Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>5. Severe</td>
<td>The impact is beyond the Stakeholders’ ability to manage or resource and as such may threaten the survival of, for example, a particular project or the company itself.</td>
<td>&gt; R10 Mil</td>
<td>Suspension of business</td>
<td>Systems unavailable for more than 2 days</td>
</tr>
<tr>
<td>4. Major</td>
<td>The impact would threaten the ability to achieve the Product and/or Organisational objectives in the medium term.</td>
<td>R2 Mil to R10 Mil</td>
<td>Adverse media coverage that has a long term impact on the Company’s image, significant brand damage</td>
<td>Systems unavailable for more than 5 hours less than 2 days</td>
</tr>
<tr>
<td>3. Significant</td>
<td>The impact may threaten the ability to achieve the Product and / or Organisational objectives in the short term.</td>
<td>R500k to R2 Mil</td>
<td>Adverse media coverage or regulatory action or fine that has a short term reputational impact, requiring corrective action and dedicated additional resources to rectify and recover.</td>
<td>Systems unavailable for more than 30 minutes but less than 5 hours.</td>
</tr>
<tr>
<td>2. Minor</td>
<td>The impact can be absorbed within the day-to-day business running costs.</td>
<td>R50k to R500k</td>
<td>Breakdown in control but minor effect on process performance</td>
<td>Systems unavailable for more than 5 minutes but less than 30 minutes.</td>
</tr>
<tr>
<td>1. Insignificant</td>
<td>The impact has little or no effect on the day to day running costs of the business.</td>
<td>&lt; R50k</td>
<td>Breakdown in control but process performance unaffected.</td>
<td>Systems unavailable for less than 5 minutes.</td>
</tr>
</tbody>
</table>
14.4 RISK LIKELIHOOD

Similarly, the criteria for the likelihood of a risk event will need to be defined and approved by the Board. The criteria for the each company could vary according to the risk tolerance agreed by the Board.

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
<th>Probability of occurrence in the next 12 months</th>
</tr>
</thead>
<tbody>
<tr>
<td>5. Almost Certain</td>
<td>Expected to occur in most circumstances or occurs regularly.</td>
<td>&gt; 70%</td>
</tr>
<tr>
<td>4. Likely</td>
<td>Occurrence is noticeable, starting to be of nuisance value.</td>
<td>40% to 70%</td>
</tr>
<tr>
<td>3. Possible</td>
<td>Occurs occasionally.</td>
<td>20% to 40%</td>
</tr>
<tr>
<td>2. Unlikely</td>
<td>Occurs Infrequently.</td>
<td>5% to 20%</td>
</tr>
<tr>
<td>1. Rare</td>
<td>Only Occurs in exceptional circumstances.</td>
<td>&lt; 5%</td>
</tr>
</tbody>
</table>

Fig 5.4

14.5 RISK MITIGATION

The next step in the Risk Management Process is Risk Mitigation and for this we consider an extract from the definition – viz. *with a view to avoiding, eliminating, accepting or reducing the business’s exposure to risk.*

The four risk mitigation actions are the following:

- **Avoiding the risk** to avoid the risk, a business would need to transfer the risk to another party, e.g. insuring against the risk.

- **Eliminating the risk** to eliminate the risk, a business would need to exit from the aspect of the business that is causing the risk, e.g. manufacturing risk on a specific product could be eliminated if the business discontinues the manufacture of the product and either exits from the market or procures the item required from an alternative manufacturer.

- **Accept the risk** a business may decide to accept the risk where the impact of the risk is determined to be less that the cost of controlling the specific risk

- **Reduce the Business’**
exposure to the Risk this would be achieved by introducing internal controls that either reduce the likelihood of the risk occurring or reduce the impact of the risk occurrence.

14.6 INTRODUCING CONTROL

Definition of Control: Controls are the actions taken to prevent an event from occurring or an action taken that reduces the impact of the risk event.

The introduction of control leads to two concepts of risk. These are:

- **Inherent Risk:** (Pre-Control) a subjective measure of the threat of a risk based on its inherent likelihood and inherent impact measures, without considering the effectiveness of controls, even if they exist. This produces a score that indicates the worst-case exposure in the event that there are no controls in place, or the controls fail to take effect during a risk event.

- **Residual Risk:** (Post Control) a subjective measure of the threat of a risk based on its residual likelihood and residual impact measures, giving the remaining level of risk after risk treatment measures have been taken. Residual risk can only be claimed if the controls are in place and work to reduce the risks and/or consequences to the level that is expected.

Each of these concepts of risk has different applications and is traditionally seen to impact on different sets of management or management functions.

Residual risk measures the level of risk after the portfolio of internal controls set by top management have been applied and are operating as planned. This residual risk is primarily the concern of management tasked with the Risk Management Process, as they will need to examine the residual risk, determine if this is acceptable and if not determine what additional action needs to be taken, e.g. introducing additional controls, securing insurance to counteract the residual risk, or recommending to the Board that the specific operation causing the risk be ceased.

Inherent Risk is used by Operational Management and Internal Audit to determine where they need to be focusing their attention. Once the internal controls have proved that they do effectively reduce the risk to the residual level, Operational Management often take their eye off the risk as they have satisfied themselves that the risk event would be prevented. However, this is dependent on the lower management, supervisors and staff actually performing the controls effectively and consistently. Also, this does not take into account deliberate sabotage to fraudulent actions. This is where Internal Audit comes into play. They will assist management to ensure that their “Good Faith” assumption is working and that the controls are being effectively, efficiently and consistently applied.
### 14.7 Risk Assessment and the Risk and Control Framework

The risk analysis (mentioned in 5.2 above) would need to be done twice for each Risk, firstly without any control, to determine the Inherent risk and secondly taking into consideration all the controls in place, to determine the Residual risk.

There are multiple ways in which to perform the Risk Assessments, some of these being:

- **Risk Management workshops** – the Risk Manager would need to determine who the effective players are in each business process and would then need to get there parties around a table and facilitate a discussion on the risk and its associated control, culminating in a vote and a determination of the Impact and Likelihood of each risk event, pre and post control.

- **Risk Management Questionnaires for assessment and collation** – This is less invasive as each party identified by the Risk Manager, would be sent a questionnaire and asked to complete this at their own pace / time. Then these would be collated, the scores averaged out and summarised to form the final assessment. Where the rating scores for the impact and likelihood are greatly disparate, discussion would be required to finalise the risk ratings.

To be able to do this effectively, and in a formal assessment as required by King III, it becomes necessary to document all the risks and the controls that are in place to mitigate the risk. Attached below (see Figure 5.5 below) is an example of a risk assessment document used to conduct the workshops.
King III refers to a Risk and Control framework, as a part of the formal Risk Assessment process. Simply put, this is the compilation of the documents that are prepared for the Risk Assessment workshops or questionnaires.

In the example above (see Figure 5.5) a Systems Manual reference is used to arrange the questionnaires in a formal structure, arranging the risks by Risk Category, Business Area and Business Process.

The columns that are headed by Green could be delegated to the Internal Audit department to document as this would save valuable management time.

As the workshops would take some time to complete, Internal Audit could allocate their own Risk Exposure rating initially to allow them to conduct risk based audits while the risk management process is rolling out.
15. KING III AND THE RISK MANAGEMENT PROCESS

15.1 WHO IS RESPONSIBLE FOR RISK MANAGEMENT

King III Report on Governance for South Africa – 2009 defines 10 Principles for Risk Management, in Chapter 4 – the Governance of Risk. These can be summarised as:

1. The Board should be responsible for the governance of risk.
2. The Board should determine the levels of risk tolerance.
3. The Risk Committee or Audit Committee should assist the Board in carrying out its risk responsibilities.
4. The Board should delegate to Management the responsibility to design, implement and monitor the Risk Management Plan.
5. The Board should ensure that risk assessments are performed on a continual basis.
6. The Board should ensure that frameworks and methodologies are implemented to increase the probability of anticipating unpredictable risks.
7. The Board should ensure that management considers and implements appropriate Risk Responses.
8. The Board should ensure continual risk monitoring by management
9. The Board should receive assurance regarding the effectiveness of the risk management process.
10. The Board should ensure that there are processes in place enabling complete, timely, relevant, accurate and accessible risk disclosure to stakeholders.

15.2 THE BOARD’S DIRECT RESPONSIBILITY

Principle 1 - The Board should be responsible for the Governance of Risk

The Governance of Risk should be via a formal process which includes the systems and processes of risk management, documented in a Risk Management Policy and a Risk Plan.

- The Risk Policy sets the tone for risk management in the organisation and must:
  - Indicate how risk management will support the company's strategy.
  - Include the definition of Risk, Risk Management and must define the objectives of Risk Management in the Company.
  - The document must also state the Risk approach and Philosophy as well as define the responsibility and ownership of the Risk Management Process in the Company.
The Risk Plan must consider the Maturity of the Risk Management Process and must include:

- The Company's Risk Management Structure – Who is responsible for which actions.
- The Risk Management Framework – The approach to be used, e.g. COSO, ISO IRMSA or an in-house developed approach.
- The Standards and Methodology – milestones, phases, tolerances, intervals, frequencies.
- Risk Management Guidelines – Detailed guides for workshops, committees, etc.
- Integration Methods – Risk Awareness and Training Programmes
- Details of the Assurance and Review of the Risk Management Process – e.g. Internal Audit.

**Principle 2 - The Board should determine the Levels of Risk Tolerance**

As was stated earlier the Board needs to set the criteria that will be used to conduct the Risk Assessments which should include the criteria for the various levels of potential Impact and Likelihood, as well as the risk associated with the various combinations of Risk Impact and Likelihood, depicted in a Risk Matrix. An example of such a board approved "Levels of Risk Tolerance" document is attached as Figure 6.1.

![Risk Matrix Image](image-url)
Principle 3 - The Risk Committee or Audit Committee should assist the Board in carrying out its Risk Responsibilities

The manner in which the Risk Committee or Audit Committee should assist the Board in carrying out its Risk Responsibilities is the topic of a separate chapter of the Report which covers the Principle and detailed recommendations in Chapter 3 of the King III Report on Governance for South Africa – 2009.

Principle 10 - The Board should ensure that there are processes in place enabling complete, timely, relevant, accurate and accessible Risk Disclosure to Stakeholders

Principle 10 covers the Relationship with Stakeholders and the Integrated Reporting to Stakeholders. The King III report details these two topics in Chapter 8 – Governing Stakeholder Relationships, and in Chapter 9 – Integrated Reporting and Disclosure.

15.3 Management Responsibility

The Principles 4 to 8 state the 5 responsibilities that the Board should delegate to Management.

Thus Management must:

- Ensure that Risk Assessments are performed on a continual basis.
- Implement Frameworks and Methodologies to increase the probability of anticipating unpredictable risks.
- Consider and Implement appropriate Risk Responses.
- Monitor Risk on a continual basis.

While these Risk Management functions are important they must be accommodated in the life of a Manager who already has a full portfolio in running the business, meeting customer demands and operating at a profit, so where does he/ she find the time? The best approach, although at a cost, is to set up a Risk Management function, either In-house or using an outsourcing to a risk consultancy, and for management only to ensure that they are given the correct resources, access to the business, its management & staff, and to ensure that they achieve the objectives and milestones set out in the Risk Plan.

15.4 The Risk Management Function

To facilitate the Board's responsibility of Oversight, Management must provide feedback to the Board, in the form of:

- Risk Assessments - a few pages back we looked at an extract from a typical Risk Assessment which showed only 1 risk and its 5 controls, so
o Just how long would the full workshop document be, showing the 347 Risks and their associated controls?

o How long would it take to customise this list to suit your business? and

o How long would the workshop last to evaluate the inherent and residual risks of all these risks?

The simple answer is too long to do at once, and thus the Risk Plan requires the Board to set standards and a methodology, which includes milestones, phases, tolerances, intervals, and frequencies.

The industry norm in this regard is that a full Risk Assessment covering all the Business Processes should be covered in a 3-year cycle, and can be divided into Phases to be completed at appropriate Intervals, with milestones set for reporting any variances outside the set Tolerances.

- **Risk Registers** - based on the Risk Tolerances that were set by the Board Management would present the Board with a register of Risks that fall above the tolerances set.
  
  o An example of a typical risk register would be all risks that have a Residual Risk that fall within the High Risk Category on the approved Risk Matrix.
  
  o The Board may also wish to see a Risk Register of all Catastrophic Risks (Inherent Impact rated as 5), irrespective of the expected frequency of the occurrence.

- **Risk Mitigation Actions Plans** - once the Risk Assessments have been completed and the Risk Registers reflecting the Residual Risks Identified, the Board will need to be informed what is going to be done to address these Residual Risks, starting with High Risks.
  
  o This will be typically done in the Risk Mitigation Action Plan, together with Monthly Progress reports to the Board on progress against the Action Plans.

- **Monitoring & Corrective Action Reports** - once the Risk Assessments have been completed and risks requiring on-going monitoring identified, monthly monitoring and corrective action reports would be required by the Board (e.g.)
  
  o In our example of the Risk Register of Catastrophic Inherent Impacts a typical event would be a Dust Explosion. This is where the dust build-up inside a silo reached a certain density and if then ignited by a spark from something as simple as an old conveyer belt scraping against metal, causing an explosion. This type of explosion has historically happened once every 20 years somewhere in the world. If such an event should occur in Durban Harbour, every building in a radius of 20km would be devastated (up to Umhlanga Rocks). However this can be controlled and these controls need to be closely monitored.
15.5 The Role of Internal Audit

**Principle 9 - The Board should receive assurance regarding the effectiveness of the Risk Management Process.**

In the past Internal Audit was also responsible for the implementation of the Risk Management Plan, but King III has recommended that the Risk Management function be split from Internal Audit to enable Internal Audit to be more effective and independent in their assessment of the Risk Management Process.

King III Report on Governance for South Africa defines 5 Principles for Internal Audit, in Chapter 7 – the need for and Role of Internal Audit. These can be summarised as:

1. The Board should ensure that there is an effective risk based Internal Audit.
2. Internal Audit should follow a risk based approach to its plan.
3. Internal Audit should provide a written assessment of the effectiveness of the Company’s Systems of Internal Control and Risk Management.
4. The Audit Committee should be responsible for overseeing Internal Audit.
5. Internal Audit should be strategically positioned to achieve its objectives.

Of the 5 Principles in the King III Report for Internal Audit, only two are relevant from a Risk Management point of view. These are:

**Principle 1 - The Board should ensure that there is an Effective Risk Based Internal Audit.**

While Risk Management is considering the Residual Risk, Operational Management are responsible for ensuring that the controls that reduce an **Inherently High Risk** to acceptable levels of Residual Risk are being complied with.

Internal Audit assist Operational Management with this Internal Control Process by verifying that the Controls in place to reduce the Exposure to Inherently High Risks:

- Are Effective and Adequate to Mitigate the Risk, and
- Are being effectively and consistently applied in all business processes, in all business locations, at a frequency that is aligned with the relevant size and risk profile of each business Unit.

**Principle 3 - Internal Audit should provide a written assessment of the effectiveness of the Company’s Systems of Internal Control and Risk Management.**

Based on the Risk Based verification of Internal Control, Internal Audit will report to the Board, via the Audit Committee, on the Effectiveness of and Level of Compliance to the Internal Controls documented in the Risk Management Process.
In addition to this traditional role for Internal Audit, they have also been tasked to assess and report on the effectiveness of the entire Risk Management Process, thus effectively the 5 principles, which we labelled Management Responsibility.

However effective reporting is almost impossible unless the Board ensures the independence of the Internal Audit Function.
16. INFORMATION TECHNOLOGY RISK

King III Report on Governance for South Africa defines 7 Principles for IT Governance, in Chapter 5 – the Governance of Information Technology (IT). These can be summarised as:

1) The Board should be responsible for Information Technology (IT) Governance
2) IT should be aligned with the performance and sustainability objectives of the Company.
3) The Board should delegate to management the responsibility for the implementation of an IT Governance Framework
4) The Board should monitor and evaluate significant IT Investments and Expenditure
5) IT should form an Integral part of the Company’s Risk Management.
6) The Board should ensure that Information Assets are managed effectively.
7) A Risk Committee and Audit Committee should assist the Board in carrying out its IT responsibilities.

16.1 The Governance of IT

**Principle 1 - The Board should be responsible for Information Technology (IT) Governance.**

For the Board to effectively discharge its duties for IT Governance the following should be considered for the Agenda of the Board / Risk Committee Meeting (based on the COBIT Standards- refer to s 16.2 below)

**Annual / Twice-a-Year**

- The Role of IT in achieving the business strategy (IT Strategy).
- Technology trends, infrastructure trends, legal and regulatory environment trends.
- IT Investment and prioritisation.
- IT threat analysis and the risk profile.
- Dependency on Key Personnel and Succession planning.
- Future capacity planning (aligned with IT Strategy).
- Re-evaluation of off-site storage.
- Software Licensing.
- Clean power and backup power issue.
- Adequacy of IT Policies and amendment thereto.

**Quarterly / Monthly**

- Achievement of IT Strategy and IT Governance.
- IT performance.
- IT problems, complaints (logs) and trends, cause and actions taken to correct the incident and to prevent re-occurrence.
- Systems Development - The progress and the achievement of the Project (tactical) plans for the IT project.
- IT supplier risk and effective service delivery (measuring against SLA’s and OLA’s).
- Capacity and performance management review (historical).
- Capacity and performance challenges due to planned work pressure (future).
- Security Incidents and appropriate action taken.

**Principle 2 - IT should be aligned with the performance and sustainability objectives of the Company.**

The manner in which the Board deals with IT Governance is very similar to Risk Management, with the strategic oversight being retained by the Board and the implementation of the process being delegated to Management.

**Principle 4 - The Board should monitor and evaluate significant IT Investments and Expenditure**

The monitoring of expenditure and the effective management of IT assets is no different to that of other Fixed Assets, other than the relatively high cost of IT infrastructure.

Under principle 1, various suggested agenda items support the Board's responsibility for monitoring and evaluation IT investment and expenditure.

**16.2 The Impact of Information Technology on Risk**

**Principle 3 - The Board should delegate to management the responsibility for the implementation of an IT Governance Framework.**

The Board should make the decision on which IT Governance Framework should be implemented to ensure that Information Technology is aligned with, and able to support the Company's performance and sustainability goals.

The most common IT Governance Framework is the **COBIT standards** (Control Objectives for Information and Related Technology) as this framework is scalable and allows the level of Control and Formality to be aligned with the relevant importance and dependence on the IT infrastructure (Maturity). The maturity assessment of this framework is the key to ensuring that there is not over control and thus a waste of costs, time and effort. It is recommended that, similar to the Risk Management function, the maturity assessment and the Guidance on the Implementation of an IT Governance Framework are left to an IT Specialist, either in-house or via an outsourced consultancy.
Principle 5 - IT should form an Integral part of the Company’s Risk Management.
Although IT Risk was shown as a separate Risk Category on the Risk Universe, its assessment should form part of the Company’s Risk Management Process, and not be a separate Risk Process.

- **IT Risk should form part of the Company’s Risk Management Activities and Considerations.**
  IT Risk should form part of the Company’s Risk Management Assessment Mechanisms (Workshops) and should be handled by the same Risk Management Function as the rest of the Company, although some specialised skills may need to be obtained or contracted for the IT Function.

- **IT Management needs to ensure that they can demonstrate adequate business resilience.**
  It is Imperative that IT management ensures not only that they have Disaster Recovery Plans for the Company’s IT systems, but that these are tested regularly and that they are able to demonstrate to the Board adequate business resilience.

- **Companies must comply with applicable IT laws, rules, codes and standards.**
  Companies must comply with applicable IT laws, rules, codes and standards in all countries in which they trade and with which they do business. Various countries have different rules on what data may be held and transmitted across borders, and simple ignorance of the differences in Laws, Rules and Standards may make the Company guilty of an offence in terms of these regulations.

- **The Board must consider how IT could be used to aid the Company in the Management of Risk.**
  There are numerous IT systems available for risk management, especially in highly technical areas such as Banking and Insurance, but management must first ensure that they are clear as to the objectives and the maturity of their Risk Management process. In most small to medium enterprises, Risk Management can be done just as effectively using spread sheets developed for this purpose as with major and expensive risk management programs.

Principle 6 - The Board should ensure that Information Assets are managed effectively.
Information management initiatives are often driven by external regulations, requirements and concerns about data privacy, information security and legal compliance. To achieve compliance with external regulations, formal processes should be in place to manage information. This encompasses:

- The protection of Information (Information Security) – The Board should oversee the information security strategy and delegate and empower management to implement the strategy, ensuring that an Information Security Management System (ISMS) is developed,
implemented and recorded in an appropriate and applicable information security framework, which should include:
- Ensuring the confidentiality of information.
- Ensuring the integrity of information.
- Ensuring the availability of information and information systems in a timely manner.

- **The Management of Information (Information Management)** – The Board should ensure that there are systems in place for the management of information assets, including:
  - Ensuring the availability of information and information systems in a timely manner.
  - Implementing a suitable information security management program.
  - Ensuring that all sensitive information is identified, classified and assigned by using appropriate handling criteria.
  - The Management of the risks associated with information and information systems
  - Establishing processes to ensure continuous monitoring of all aspects of information
  - Establishing processes to ensure the maintenance and monitoring of data quality.
  - Establishing a business continuity program addressing the company’s information and recovery requirements, and ensuring the program is still aligned with the successful execution of the business’ activities

- **The Protection of personal information Processed by Companies (information Privacy)** – The Board should ensure there are systems in place for personal information to be treated by the company as an important business asset and that all ‘personal information’ possessed by the company is identified and processed according to applicable laws, such as:
  - **Regulation of Interception of Communications and Provision of Communication-Related Information Amendment Act**, [No. 21 of 2010], Assented to 3 December 2010
  - **Protection of Personal Information Bill** (As introduced in the National Assembly (proposed section 75); explanatory summary of Bill published in Government Gazette No. 32495 of 14 August 2009)

**Principle 7 - A Risk Committee and Audit Committee should assist the Board in carrying out its IT responsibilities**
The use of the Risk and Audit Committees to assist in the oversight of the IT Function is similar to their role in Risk Management and is the topic of a separate chapter of the Report which covers the Principles and detailed recommendations in Chapter 3 of the King III Report on Governance for South Africa – 2009.
17. COMPLIANCE RISK

King III Report on Governance for South Africa – 2009 defines 4 Principles for Compliance Risk, in Chapter 6 – Compliance with Laws, Rules, codes and standards. These can be summarised as:

1. The Board should ensure that the Company complies with all applicable laws and considers adherence to non-binding rules, codes and standards.
2. The Board and each individual Director should have a working understanding of the effect of the applicable laws, rules, codes and standards on the company and its business.
4. The Board should delegate to Management the implementation of an effective Compliance Framework and Process.

17.1 How Compliance Impacts on Ethics, Risk, Fraud and Governance

Principle 1 - The Board should ensure that the Company complies with all applicable laws and considers adherence to non-binding rules, codes and standards

Quite simply – the Company must comply with all applicable Laws – However the difficulty is in identifying which laws are applicable. Furthermore, exceptions permitted in the law and shortcomings of the law that presents an opportunity for abuse, which is contrary to the spirit, intent and purpose of the law, as well as proposed changes expected in legislation and regulations, should be handled in an ethical and responsible manner.

Principle 2 - The Board and each individual Director should have a working understanding of the effect of the applicable laws, rules, codes and standards on the company and its business

To fulfil its responsibility to ensure the identification of laws, rules, codes and standards the Board should ensure that there is a formal process to assess their applicability, to continually inform the Board of the applicable laws, rules, codes and standards, including changes to them. Directors should be provided training and education, as part of their induction and on an on-going basis, on the general content of applicable laws, rules, codes and standards to enable them to discharge their fiduciary duties in the best interests of the Company.

Principle 3 - Compliance Risk should form an integral part of the Company’s Risk Management Process.

Compliance risk can be described as the risk of damage, arising from non-adherence to the Laws and Regulations, to the company’s business model, objectives, reputation, going concern, stakeholder relationships or sustainability.
All these topics that should be addressed, and many more, have been addressed in the Risk Universe discussed earlier. The only additional consideration when addressing Compliance would be to ensure that the compliance risks have been considered and the controls necessary to ensure compliance have been added into the portfolio of internal controls.

**Principle 4 - The Board should delegate to Management the implementation of an effective Compliance Framework and Process**

As was discussed under Risk Management, all Risks should be analysed and documented in the Risk Universe (Risk and Control Framework) addressing the Risk Exposure, Process, Internal Controls and Standards.

This should include the risk of damage, arising from non-adherence to the Laws and Regulations under each business process individually.
18. FRAUD

Fraud is not new but it is worse than last year and will probably be still worse next year.

“Fraud and deceit abound now more than ever before”

Sir Edward Coke (1602)

18.1 Definition of Fraud

There is no single accepted definition of fraud.

It is impossible to provide a comprehensive definition of fraud. However, all definitions have one thing in common - an element of dishonesty or deceit.

Defrauding people or entities of money or valuables is a common purpose of fraud, but there have also been fraudulent "discoveries", e.g., in Science, to gain prestige rather than immediate monetary gain.

There are many dictionary definitions of the word 'fraud'; each is similar but not exactly the same. Here are some of the elements of these descriptions:

- Unfair advantage by unlawful or unfair means;
- Knowingly making a false representation;
- Intentional deception resulting in injury to another person;
- Something intended to deceive; deliberate trickery intended to gain an advantage;
- An intentional perversion of truth; deceitful practice or device resorted to with intent to deprive another of property or other right;
- The intentional and successful employment of cunning, deception, collusion; or artifice used to cheat or deceive another person whereby that person acts upon it to the loss of his property and to his legal injury;
- The act of leading a person to believe something which you know to be false in a situation where you know the person will rely on that thing to their detriment;
- A deception, intended to wrongfully obtain money or property from the reliance of another on the deceptive statements or acts, believing them to be true;
- The intentional perversion of the truth in order to mislead someone into parting with something of value;
Fraud is a crime, and also a civil law violation.

However for the purposes of this Handbook, we will use the following Definition:

**Fraud** is intentional deception to cause a person to give up property or some lawful right or to damage another individual using deceit, trickery or cheating.

### 18.2 Definition of Corruption

**Simply Put:**

Corruption is the abuse of entrusted power for private gain. It hurts everyone who depends on the integrity of people in a position of authority.

The Corruption Act, Act No. 12 of 2004: Prevention and Combating of Corrupt Activities Act, Defines Corruptions as follows:

3. 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 her self 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.
   
   (v) is guilty of the offence of corruption

*(CHAPTER 2 - OFFENCES IN RESPECT OF CORRUPT ACTIVITIES)*

*(Part I: General offence of corruption)*
18.3 Key Drivers in the Current Economic Climate

One of the Key Drivers for Fraud is ‘PEER INFLUENCE/ PEER PRESSURE’.

If the Politicians and Government not only in South Africa, but around the world are open to Corruption, then why not me?

What’s Good for the Goose is Good for the Gander

To better understand what drives the prevalence of Fraud in the Current Economic Climate, let us look at the statistics released by Transparency International – The global coalition against Corruption.

One of the statistics that they present, based on their 2011 Survey, is the Corruption Perception Index which ranks countries / territories based on how corrupt a country’s public sector is perceived to be. It is a composite index, drawing on corruption-related data from expert and business surveys carried out by a variety of independent and reputable institutions.

The other Statistic that we will be looking at is the Corruption Score, with Scores ranging from 0 (Highly Corrupt) to 10 (Very Clean)

The Remaining Data that is given on each country is supplied by the World Bank.
Below we show the rating of **South Africa**, 
As well as the **Three Giants** that we wish to be compared to: 
  o The United Kingdom, the United States and Australia.
Then three of our **Trading Partners** 
  o Brazil, Nigeria and China
And finally our **Closest Neighbours**
  o Namibia, Botswana, Zimbabwe and Mozambique.

<table>
<thead>
<tr>
<th>South Africa</th>
<th>POPULATION (2010): 50 MILLION</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>* GDP (2010): $363.7 BILLION</td>
</tr>
<tr>
<td></td>
<td>* INFANT MORTALITY RATE (PER 1,000 LIVE BIRTHS - 2010): 40.7</td>
</tr>
<tr>
<td></td>
<td>* LIFE EXPECTANCY (2009) 51.61 YEARS</td>
</tr>
<tr>
<td></td>
<td>* LITERACY RATE (2007) 88.7%</td>
</tr>
</tbody>
</table>

**Corruption Perception Index (2011)**

<table>
<thead>
<tr>
<th>Ranking</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>64 / 183</td>
<td>4.1 / 10</td>
</tr>
</tbody>
</table>

0 (Highly Corrupt) to 10 (Very Clean)

**Other Statistics for South Africa**

Percentage of people who feel the government's efforts to fight corruption are:
30% Ineffective
0% Neither Effective nor ineffective
70% Effective

Percentage of people who feel that from 2007-2010, the government's anti-corruption efforts have:
62% Increased
14% stayed the same
24% decreased
### The Three Giants

<table>
<thead>
<tr>
<th>United Kingdom</th>
<th>Corruption Perception Index (2011)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>POPULATION (2010):</strong> 62.2 MILLION</td>
<td><strong>Ranking</strong> 16 / 183</td>
</tr>
<tr>
<td><strong>GDP (2010):</strong> $2.25 TRILLION</td>
<td><strong>Score</strong> 7.8 / 10</td>
</tr>
<tr>
<td><strong>INFANT MORTALITY RATE (PER 1,000 LIVE BIRTHS - 2010):</strong> 4.6</td>
<td>0 (Highly Corrupt) to 10 (Very Clean)</td>
</tr>
<tr>
<td><strong>LIFE EXPECTANCY (2009):</strong> 80.05 YEARS</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>United States of America</th>
<th>Corruption Perception Index (2011)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>POPULATION (2010):</strong> 309.1 MILLION</td>
<td><strong>Ranking</strong> 24 / 183</td>
</tr>
<tr>
<td><strong>GDP (2010):</strong> $14.59 TRILLION</td>
<td><strong>Score</strong> 7.1 / 10</td>
</tr>
<tr>
<td><strong>INFANT MORTALITY RATE (PER 1,000 LIVE BIRTHS - 2010):</strong> 6.5</td>
<td>0 (Highly Corrupt) to 10 (Very Clean)</td>
</tr>
<tr>
<td><strong>LIFE EXPECTANCY (2009):</strong> 78.09 YEARS</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Australia</th>
<th>Corruption Perception Index (2011)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>POPULATION (2010):</strong> 22.3 MILLION</td>
<td><strong>Ranking</strong> 8 / 183</td>
</tr>
<tr>
<td><strong>GDP (2009):</strong> $924.84 BILLION</td>
<td><strong>Score</strong> 8.8 / 10</td>
</tr>
<tr>
<td><strong>INFANT MORTALITY RATE (PER 1,000 LIVE BIRTHS - 2010):</strong> 4.1</td>
<td>0 (Highly Corrupt) to 10 (Very Clean)</td>
</tr>
<tr>
<td><strong>LIFE EXPECTANCY (2009):</strong> 81.54 YEARS</td>
<td></td>
</tr>
</tbody>
</table>
## Trading Partners

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Brazil</td>
<td>194.9 MILLION</td>
<td>$2.09 TRILLION</td>
<td>17.3</td>
<td>72.76 YEARS</td>
<td>90%</td>
<td>73 / 183</td>
<td>3.8 / 10</td>
<td>0 (Highly Corrupt) to 10 (Very Clean)</td>
<td></td>
</tr>
<tr>
<td>Nigeria</td>
<td>158.4 MILLION</td>
<td>$193.67 BILLION</td>
<td>88.4</td>
<td>50.95 YEARS</td>
<td>60.8%</td>
<td>143 / 183</td>
<td>2.4 / 10</td>
<td>0 (Highly Corrupt) to 10 (Very Clean)</td>
<td></td>
</tr>
<tr>
<td>China</td>
<td>1.3 BILLION</td>
<td>$5.93 TRILLION</td>
<td>15.8</td>
<td>73.06 YEARS</td>
<td>94%</td>
<td>75 / 183</td>
<td>3.6 / 10</td>
<td>0 (Highly Corrupt) to 10 (Very Clean)</td>
<td></td>
</tr>
</tbody>
</table>
## Closest Neighbours

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Namibia</td>
<td>2.3 MILLION</td>
<td>$12.17 BILLION</td>
<td>29.3</td>
<td>61.62 YEARS</td>
<td>88.5%</td>
<td>Ranking 57 / 183, Score 4.4 / 10</td>
</tr>
<tr>
<td>Botswana</td>
<td>2 MILLION</td>
<td>$14.86 BILLION</td>
<td>36.1</td>
<td>53.01 YEARS</td>
<td>84.1%</td>
<td>Ranking 32 / 183, Score 6.1 / 10</td>
</tr>
<tr>
<td>Zimbabwe</td>
<td>12.6 MILLION</td>
<td>$7.47 BILLION</td>
<td>50.9</td>
<td>48.45 YEARS</td>
<td>91.9%</td>
<td>Ranking 154 / 183, Score 2.2 / 10</td>
</tr>
</tbody>
</table>
As can be seen from the statistics, South Africa has a long way to go to Combat Perceived Corruption in the Government, but the people of South Africa feel that things are improving.

The time to Combat Corruption and Fraud in the workplace ...... Is NOW!
19. FACES OF FRAUD AND CORRUPTION

From amongst the many faces of fraud, we have chosen to focus on the following four:

19.1 Asset Misappropriation

The most commonly occurring fraud within corporations is asset misappropriation. According to the Association of Certified Fraud Examiners, based on their international survey conducted (including South Africa), more than 91% of all internal fraud schemes involved an asset misappropriation element, and the median loss from an asset misappropriation was R1.2 Million ($150,000). Asset misappropriations include the misuse or theft of assets belonging to a company.

These are the white collar crimes we think about most, probably because they are so commonplace in terms of the number of cases that occur. Furthermore, they are the kinds of cases we most commonly hear about in the press.

Asset misappropriations are commonly detected through management supervision, either via direct oversight or management checks and balances, or through indirect methods such as internal controls like segregation of duties, account reconciliation, and independent verification of data.

Many instances of errors and fraud can be detected through normal control activities (like account reconciliation) in conjunction with analytical review of accounts (such as ratio analysis). Additional things such as Data Analytics (analysis of computerised data with specialized software) can aid in detecting asset misappropriation.

Tips and Techniques

Techniques to monitor or detect asset misappropriation:
- Customer returns, credits or write-offs
- Unallocated payment / Suspense accounts
- Inventory scrap, spoilage, obsolescence
- Inventory shrinkage
- Fixed asset write-offs

Techniques to prevent asset misappropriation:
- Employee monitoring via CCTV or Management-by-walk-about
- Segregation of duties
Examination and countersigning of documentation
Examination of cancelled cheques
Independent verification
Surprise audits
Job rotation
Physical security

19.2 Financial Misstatement

A valuation is only as accurate as its underlying financial data.

Some unscrupulous business owners employ creative accounting techniques to hide assets and lower profits, or to inflate assets to increase profitability and improve the Statement of Financial Position (Balance Sheet) of the Company

When these smoke-and-mirror tactics go undetected, they alter the company's appraised value. Financial misstatement to decrease business value is especially common when the business is involved in contentious litigation, such as an oppressed minority shareholder case. Financial misstatement to increase business value is used when the company is considering financing or investment or when profitability is used to set bonuses or perks, such as incentive trips. Although not exhaustive, the following list outlines some of the common ways deceitful controlling shareholders can massage the numbers:

Misreporting revenues or expenses - Revenues and their corresponding expenses should be “matched” in the reporting period in which they were earned or incurred. But if an owner delays revenue recognition or accelerates expense recognition, he or she will artificially lower profits in the current accounting period. Likewise if the owner uses pre-invoicing or delays expense recognition (e.g. capitalises expenses) he or she will artificially inflate profits in the current accounting period.

Failing to properly adjust owners’ compensation and related-party transactions - Owners’ compensation is among the most common valuation adjustments. By comparing an owner’s compensation to industry benchmarks or various compensation studies, the valuator can assess whether it appears reasonable. Valuators also identify related parties and evaluate whether related-party transactions, such as rental payments and management fees, occur at arm’s length.

Mishandling of business expenses - Many private business owners treat their company’s cheque accounts as their own personal accounts. For instance, the business might fund the owner’s legal fees or excessive meals and entertainment. This is especially prevalent in companies where the
management benefits have been reduced over time or where the management used to be owners in corporate takeovers.

**Mishandling of quasi-business assets** - On the other hand, owners sometimes report personal assets, such as art collections or vacation homes, on their companies’ balance sheets. Like other non-operating assets, these items (and, if applicable, their corresponding income and expenses) should be isolated. The valuator then makes a last-minute adjustment to his or her value conclusion for the fair market value of the quasi-business asset.

Parties who suspect foul play should discuss these concerns with their valuators. Scorned spouses, disgruntled managers and minority shareholders are especially helpful at directing valuators to the specific assets or expenses that controlling shareholders have manipulated.

### 19.3 Computer Crime

**Computer crime** refers to any crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. **Netcrime** refers to criminal exploitation of the Internet. **Cybercrimes** are defined as: “Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)”.

Issues surrounding this type of crime have become high-profile, particularly those surrounding cracking, copyright infringement, child pornography, and child grooming. There are also problems of privacy when confidential information is lost or intercepted, lawfully or otherwise.

Such crimes may threaten a nation’s security and financial health. Internationally, both governmental and non-state perpetrators engage in cybercrimes, including espionage, financial theft, and other cross-border crimes. Activity crossing international borders and involving the interests of at least one nation state is sometimes referred to as cyber warfare. The international legal system is attempting to hold perpetrators accountable for their actions through the International Criminal Court.

it is natural that you would want to avoid being such a victim, and there are a number of things you can do to protect yourself and your family. If you use a computer, you’re vulnerable to malware. And if you are vulnerable to malware, you are enabling crime on a mass scale.

Malware refers to viruses, trojans, worms and other software that gets onto your computer without you being aware it’s there. Back in the early part of the century, most such malware’s primary aim was thrill. The people writing the software found it amusing to write a program that exploits security flaws just to see how far it could spread.
Today the incentive for making such software is generally more sinister and the reason it makes the list of the top five computer crimes. In some cases a piece of malware will pretend to be a legitimate piece of software, and will ask you for money to remove it. Never, ever give money to programs you don’t remember buying.

Not all malware tries to extract money from you directly, however. Many simply imbed themselves into your computer in order to make use of it. This sort of network is referred to as a botnet, and is a key tool of the trade for a number of Internet crimes. Black-hat hackers may intend to launch an attack against a government or institution, and will use a network of compromised machines to do so.

Of course, whatever the motivation, such software is a drain on your computer’s resources so it’s best to be protected against it.

Just as important is, don’t download software from sites you’re not sure you can trust, regardless of what operating system you run. Avoid pirated software, it may seem like a good way to save money, but frequently you’re also getting some malware thrown in.

In general, just use common sense before opening any sort of file, because you don’t want to compromise your system.

19.4  Identity Theft

Identity theft is quite possible without the use of a computer by observation, dumpster diving (sorting through your trash) and undetected invasion of your house and office, but the most common manner is via your computer and your internet usage.

Thus Identity theft easily makes the list of the top five computer crimes. In America alone there are almost 9 million victims of identity theft every year. The concept is simple; someone gains access to your personal information and uses it for their own benefit. This could range from a black-hat hacker stealing your online banking account login and password to getting access to your identity number and using it to pretend to be you. Such people can make themselves a lot of money with your personal information, and destroy your credit rating and standing in the process.

Never connect to your bank account on a public computer, or using a WiFi access point you’re not absolutely sure you can trust. The same goes for using your credit card or any other on-line payment mechanism to pay for something.

Never use your credit card at a site you are not sure you can trust.
The most important thing is to never share any personal information – such as your bank account number, your Identity number or any information a fraudster could use to steal your identity – in an email, instant message or any other form of unencrypted communication. None of these communication channels were designed to be secure, and as such are not the proper way to share such information.

If you get an email from your bank, your credit card company, eBay or any other service with access to financial information asking you to “update your personal information” ignore it. This is a common ploy used by fakers. No Bank will ever request you to provide or confirm personal data over the web or the phone. Make sure you are very familiar with the interface of all such sites, because fakers can severely take advantage of you if you are not careful.
20. REDUCING FRAUD RISK

20.1 Understanding your Fraud Risk

When we looked at Risk and Risk Management, we referred to identifying the risks associated with each business process that would prevent one from achieving that process’ objectives. You would have identified the business based risks associated with error, omission, uneconomical use of resources, lack of understanding, etc. One other category of risk that should also have been considered is Fraud Risk.

But, what do we mean by Fraud Risk.

This is the possibility that an employee or a third party will intentionally cause an error or an omission in exercising the controls which have been put in place to mitigate the risk. So while the internal controls would, under normal circumstances, be adequate to mitigate the risk, by preventing the risk event or detecting the risk event if it has occurred, fraud brings in another dimension. That dimension is the purposeful sabotaging of the controls or omission of control procedures to enable the removal of assets, the embezzlement of funds and to prevent these frauds from being detected.

A further dimension of fraud is collusion. This is even more difficult to protect against as the internal controls, such as segregation of duties that prevent any one person from being able to control or influence all the steps in a process, thus preventing the fraud, are bypassed by two or more people working together. This can only be protected by adding additional layers of control, and this could lead to over-control under normal circumstances.

20.2 HARDENING YOUR CONTROLS AGAINST FRAUD

As the preventative controls are sidestepped, additional controls will need to be added or existing controls enhanced to prevent or at least detect the fraud occurrence. The most effective manner of preventing purposeful omission of controls is to automate these controls. An example of this is demonstrated by the following scenario:

The control process is that the teller must inspect the Identity document of the customer before accepting a payment by cheque. However, if this is not done and the omission is not observed by the till controller that, under normal circumstances has to control up to 6 tills, the omission cannot be detected after the fact. One of the additional controls that can be implemented to prevent unintentional omission is to record the ID number on the back of the cheque, but this opens the business to all sorts of
additional risk from security of data in their possession viz. the ID number and the possibility of Identity theft. An alternative control is to put a step in the till operation where the system requests the till operator to answer the question “have you inspected the customer’s ID”. This has however also had limited success in the past as operators become familiar with the till operation and learn the sequence of buttons to push, without even reading the prompts or considering the questions being posed.

The various additional controls that could be implemented to prevent unintentional error or omission will still not harden the control against fraud. An enhanced control would be the entering the ID number into the system or, to prevent errors in data capture, moving to the scanning the ID barcode, but again the data security risk rears its head so we would then need to ensure that the system does not record the data in a readable format (as we have seen with our credit card numbers on the till slip that we sign viz. **** **** **** 2345).

An addition to fraud risk is that the cashier does not record the actual ID number but simply enters a string of numbers sufficient to fill the data field, but this can be controlled by programming in the ID Number algorithm which will test for a Valid ID Number. Thus also testing against third party fraudulent ID documents.

A detective or investigative tool that has been implemented by most large super markets is CCTV. This acts as a deterrent as the staff members are aware that if a fraudulent cheque is accepted, the CCTV recording can be viewed and it will show if they followed the cheques acceptance policy fully. Also this recording can be used in disciplinary hearings as well as identifying the perpetrator of the crime.

As can be seen by the example above hardening controls against fraud is no simple matter and will take time, forethought and experience to achieve effectively.

The difficulty with all fraud prevention steps, that can be taken, is that the cost of these steps needs to be considered and excessive control must be prevented.
21. DETECTION OF FRAUD AND FRAUD AWARENESS PROGRAMMES

21.1 Embedding Fraud Awareness in the Workplace

Possibly the best fraud prevention control is a vigilant and dedicated workforce.

Embedding fraud awareness in the workplace is not as simple as it sounds as we need to compete for time and attention against such objectives as productivity and profitability. It is very easy to identify actual occurrences of wastage by weighing or counting the damaged parts in a manufacturing plant, and thus justifying controls that prevent wastage. However, in the softer, fluffy area of fraud prevention cost justification is more difficult. It is difficult to count the incidence of fraud prevented as they did not occur, and thus management must trust that the frauds would have occurred if the additional fraud hardened controls had not been in place.

For fraud awareness to play any meaningful part in a business, the Board of Directors and top management must believe that the programme is necessary and they need to be seen to be giving it their full support.

The starting point is for all levels within the organisation to understand what fraud is and why it impacts on the company and themselves. If employees do not understand the consequences of fraud, they have less motivation to be vigilant and to report fraud to management. The old adage is “they are not stealing from me, only from the company, and that is none of my concern”.

If employees understand the impact of fraud on them directly this could change – “We will have to do away with free lunches that should cost R30 per employee as this has escalated to R70 due to fraud or theft, and this has pushed the subsidy to the point where it can no longer be afforded”.

Corruption often goes unchallenged when people do not speak out about it. Witness accounts offer invaluable insights into corruption, and are powerful tools in the fight against it. From exposing multi-million dollar financial scams to dangerous medical practices, whistle-blowers play a crucial role in saving resources and even lives.

Whistle blowers are invaluable in exposing corruption, fraud and mismanagement. Early disclosure of wrongdoing or the risk of wrongdoing can protect human rights, help to save lives and preserve the rule of law. Public education is also essential to de-stigmatise whistle blowing, so that citizens understand
how disclosing wrongdoing benefits the public good. When witnesses of corruption are confident about their ability to report it, corrupt individuals cannot hide behind the wall of silence.

21.2 Whistle Blowing – Methods

Whistle blowers are less likely to report workplace misconduct when their employers do not provide clear internal reporting channels, and in some settings, whistle blowing carries connotations of betrayal rather than being seen as a benefit to the public. Ultimately, societies, institutions and citizens lose out when there is no one willing to cry foul in the face of corruption.

There are various mechanisms that a company can put in place for whistle blowing, but these are all worthless unless supported from the Board all the way down to the shop and factory floor. The acceptance of whistle blowing as an honourable action and in fact the duty of every employee is imperative and this must be supported by actions from the Board and Top Management.

There are various mechanisms to house the whistle blowing line in-house, ranging from an answering machine with tapes reviewed by the Risk or Audit Manager, using the company’s customer hot-line to take and record calls, or even setting up a special function housed within the Personnel Department, but all these have one failing, they are seen to be internal and could be perceived as a direct line to the “management” that they may be reporting on.

Experience has shown that the use of an external hot-line consultant to launch, market, manage and operate the whistle blowing mechanism totally independent from the Company and its management is more acceptable to the average employee and the man in the street. A hot-line consultant will also ensure that the correct structure for reporting and investigating reported irregularities is put in place and that reports are sent to a manager at least one level above any person mentioned in the report, even if just in passing.

21.3 Whistle Blowing – Protection

Blowing the whistle can carry high personal risk – particularly when there is little legal protection against dismissal, humiliation or even physical abuse. Controls on information, libel and defamation laws, and inadequate investigation of whistle-blowers’ claims can all deter people from speaking out.

Safeguards also protect and encourage people willing to take the risk of speaking out about corruption. We must push companies to introduce comprehensive whistle-blower policies to support the legislation to protect those that speak out and ensure that their claims are properly investigated, and workplace reprisals against whistle-blowers should be seen as another form of corruption.
US Research of 233 whistle blowers surveyed:
- 90% either lost jobs or were demoted
- 27% subjected to law suits
- 26% required medical/psychiatric attention
- 25% became alcoholics
- 15% got divorced
- 10% attempted suicide

21.4 Protected Disclosures Act, No. 26 of 2000

This Act has been commonly referred to as the “Whistle Blowers” Act. Its provisions are potentially as effective as they are of concern.

The Whistle Blowers Act makes 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.

The Act provides for the protection of employees who make a disclosure which is protected in terms of the Act. The object to the Act is stated to...

"create a culture which will facilitate the disclosure of information by employees relating to criminal and other irregular conduct in the workplace in a responsible manner by providing comprehensive statutory guidelines for the disclosure of such information and protection against any reprisals as a result of such disclosure; promote the eradication of criminal and other irregular conduct in organs of State and private bodies”.

The Act indicates the nature of information which might form the subject of a “disclosure”, including:

a) that a criminal offence has been committed, is being committed or is likely to be committed;
b) that a person has failed, is failing or is likely to fail to comply with any legal obligation to which that person is subject;
c) that a miscarriage of justice has occurred is occurring or is likely to occur, and so on.

The topics are therefore extremely broad. The qualifications given to a “protected disclosure” requires that disclosure to be “made in good faith”. This qualification relates to the reasonable belief of, for example, the employee that the information disclosed, and any allegation contained in it, is substantially true and that the disclosure is not made for the purpose of personal gain.