Remgro Limited

Fraud, Bribery and Corruption Prevention, Detection and Response Policy

Document owner:
Deon Annandale
Reviewed February 2023

Contents

1. SCOPE OF THE POLICY

This policy applies to all Remgro employees, its subsidiaries and any third party with which Remgro does business including, but may not limited to, suppliers, consultants and independent contractors. ("suppliers").

2. POLICY STATEMENT

It is the policy of Remgro that fraud, bribery, corruption, maladministration, or any other dishonest activities of a similar nature will not be tolerated. Allegations of such activities will be investigated, where required, and actions instituted against those found responsible. Such actions may include the laying of criminal charges, civil and administrative actions and the institution of direct recoveries where applicable.

Prevention, detection, response, and investigative strategies will be designed and implemented where necessary. These will include internal controls as currently prescribed in existing policies, procedures and other relevant prescripts to the activities of the company. In addition, fraud awareness training and risk awareness on these topics will be rendered via ROTIG.

It is the responsibility of all employees of Remgro to report all incidents of suspected fraud, bribery and corruption, or any other dishonest activities of a similar nature to their managers or via the Ethics Hotline. All reports received will be treated with the requisite confidentiality and will not be disclosed or discussed with parties other than those charged with investigation into such reports.

All Managers are responsible for the detection, prevention and investigation of fraud, bribery and corruption or any dishonest activities of a similar nature, within their areas of responsibility. Where such instances could be material they should refer such allegations to the CAE for consideration given the potential technicality, burden of proof, physical risk and perceived lack of independence within the confines of a Managers area of responsibility.

3. ETHICS AND VALUES STATEMENT

Fraud and unethical behaviour represent a significant potential risk to an enterprise's assets, culture, performance and reputation.

Remgro is committed to protecting its assets, including its reputation as an enterprise led and managed by directors and senior managers who strive to uphold the highest ethical standards and values. These values are, furthermore, incorporated into all dealings by management and staff.

We will not tolerate corrupt or fraudulent activities whether internal or external to the organisation, and will vigorously pursue and prosecute any parties, both civilly and criminally, that engage in such practices or attempt to do so in our ambit of responsibility. In instances where the Remgro brand and corporate information is illicitly used by external fraudster, we will support initiatives by SAPS and/or other regulatory bodies mandated by law to investigate such instances to protect our brand and reputation. In instances where kidnap forms part of an extortion the related Remgro risk management process will be utilised given the inherent extended exposures.

4. DEFINITIONS

Fraud is defined as "the unlawful and intentional making of a misrepresentation which causes actual and or potential prejudice to another". The use of the term is in its widest possible meaning and is intended to include all aspects of economic crime and acts of dishonesty, including theft, forgery, uttering and unlawful appropriation of assets and also the omission to disclose fraud. This is extended to include inter alia other illegal or unethical acts such as market rigging and conflicts of interest or misuse of positions of authority for personal gain.

Corruption is any conduct or behaviour where a person accepts, agrees or offers any gratification for him/her or for another person where the purpose is to influence or induce said person to act (or desist from acting)

dishonestly, illegally or contrary to their designated responsibility of the interests of the company. Such behaviour also includes the misuse of material or information, abuse of a position of authority or a breach of trust or violation of duty.

5. FORMS OF CORRUPTION

The following are examples of different types of corruption. The list is not deemed exhaustive.

Bribery

Bribery involves the promise, offering or giving of a benefit that improperly influences the actions or decisions of employees.

Embezzlement and theft

This involves the withholding and/or theft of resources from/by persons who control such resources.

Fraud

Any conduct or behaviour of which a dishonest representation and/or appropriation forms an element.

Extortion and blackmail

The coercion of a person or entity to provide a benefit to an employee, another person or an entity, in exchange for acting (or failing to act) in a particular manner.

Abuse of power

The use by an employee of his or her vested authority to improperly benefit his or herself, another employee, person or entity (or using vested authority to improperly discriminate against another employee, person or entity).

Conflict of interest

The failure by an employee to act or to consciously fail to act in a matter where the employee has an interest or another person or entity that has some form of relationship with the employee has an interest. This includes the failure to disclose their interest or that of a related party when participating in decisions that do or may have an impact on the employee or related party.

Abuse of privileged information

This involves the use, by an employee of privileged information and knowledge that an employee possesses as a result of his/her office to provide unfair advantage to the employee or another person or entity to obtain a benefit.

Favouritism

The provision of services or resources according to personal affiliation of an employee.

Nepotism
An employee ensuring that family members or friends are appointed to service positions or that they receive contracts or commercial benefits.

6. RESPONSIBILITIES FOR IMPLEMENTATION OF THE POLICY

The following section outlines the fraud and corruption risk management responsibilities associated with different roles within the company, designed to prevent and detect fraud.

The Board

The Board has overall responsibility for ensuring that this Policy complies with applicable fraud and corruption related legislation and that adequate processes are put in place to ensure compliance with this Policy, as far as reasonably practicable. This includes the coordination of risk assessments, overseeing the investigation of suspected fraud and corruption, and facilitation for the reporting of such instances.

Committees

Annual fraud and corruption risk assessments to identify potential fraud and corruption risk will be conducted and presented to the ROTIG Committee by the risk management and internal audit department. Fraud Risk is furthermore reported on to the Audit and Risk Committee.

Directors / Senior Management

Senior management, under the guidance of the Board, will ensure that it does not become complacent in dealing with fraud and corruption and that it will ensure the organisation's overall fraud and corruption strategy is reviewed and updated regularly. Furthermore, senior management will ensure that all employees and stakeholders are made aware of its overall anti-fraud and corruption strategies through various awareness initiatives. Management in Remgro is responsible for ensuring those reporting to them is made aware of and understand this Policy and are given adequate and regular training.

Human Resources

The Human Resources Department is responsible for ensuring that the principles of this Policy is incorporated into all aspects of Remgro's policies, including recruitment, training, performance evaluation, remuneration and reward; and that policies are continually improved.

Finance

The Finance Department is responsible for ensuring that the principles of this Policy is incorporated into all aspects of Remgro's financial management policies, including maintaining of accurate books and record, corporate accounting, staff expenses and donations.

Employees and subsidiaries

Employees and subsidiaries are responsible for challenging instances where bribery and corruption may occur. Employees, subsidiaries, and suppliers may not give or receive bribes and are responsible for reporting all bribery and corruption that they are aware of via the procedures laid out in this Policy. It is critically important that all employees and subsidiaries notify Internal Risk and Audit Department as soon as possible if bribes are offered or requested by a third party, or where they suspect that this may happen in the future, or believe they are a victim of another form of unlawful activity.

Where employees and subsidiaries are uncertain about whether a particular behaviour or conduct constitutes bribery or corruption, or where there may be any other queries, these should be raised with Internal Risk and Audit Department.

Suppliers

Whenever suppliers are involved, in any way, with the business of Remgro, they are required to comply with the rules and procedures laid out in this Policy. For business partners that are juristic entities, the senior management of such entities are required to take reasonable practicable steps to ensure that all of their employees, agents, representatives and other persons involved with the business of Remgro on their behalf, are aware of, and comply with, the applicable rules and procedures of this Policy. This obligation on Remgro's suppliers will be facilitated via the review of approved terms of trade and service level agreements by the legal department.

7. OPERATIONAL STRATEGIES

7.1 Internal Controls

Internal controls are our first line of defence against fraud and corruption. While internal controls may not fully protect the company against fraud and corruption, they are essential preventative and detective elements in the overall Anti-fraud and Corruption Strategy.

The Audit and Risk Committee shall monitor Remgro's progress and standing regarding the legislative compliance requirements and will be the responsibility for providing independent oversight and assessment of

the adequacy and effectiveness of this Policy. Furthermore, they are responsible for ensuring that the internal audit program incorporates steps to ensure adherence to internal controls.

7.2 Prevention strategies

A number of combined initiatives result in an overall preventative environment in respect of fraud and corruption. These include the following:

7.2.1 Employee awareness

Continuous employee awareness as regards the Anti-fraud and Corruption Strategy, Code of Ethics and Code of Ethics Hotline Policy ("Whistle blowing policy"), as required by the Companies Act, is deployed to ensure that the temptation to commit any malpractice is reduced. This is further emphasised by visible ethical leadership and the maintenance of the Remgro culture.

7.2.2 Pre-employment screening

Pre-employment screening will be carried out for all key appointments, and evidence of such screening will be maintained by the HR Department.

7.2.3 Internal audit programme

A robust Internal Audit programme, which focuses on the prevalent high Fraud and Corruption risks, serves as an effective preventative and detective measure.

7.2.4 Disclosure of interests

According to procedure all directors and nominated offices are required to disclose certain information regarding their business interests on an annual basis.

7.2.5 Gifts Policy

According to this procedure all employees are required to declare gifts received, as per Remgro's Gift Policy, above the pre-determined value to ensure transparency and to monitor trends and values of gifts received.

7.2.6 Supply chain governance

Remgro requires, per agreement, that their key suppliers comply with ethical and compliance requirements including disclosure of gifts and related transfer of benefits.

7.3 Detection strategies

Detection of fraud and corruption may occur through:

- Vigilance on the part of employees, including line management;
- The Internal Audit function;
- Ad hoc management reviews;
- Anonymous reports; and
- The application of detection techniques, including supervisory controls, technology and information procedures and reporting processes.

7.4 External Audit

The Audit and Risk Committee holds an annual discussion with the external auditors to ensure that due consideration is given, by the auditors, to ISA 240 "The Auditors' Responsibility to Consider Fraud in the Audit of a Financial Statement", as revised from time to time.

8. RESPONSE STRATEGIES

8.1 Reporting fraud and corruption – Remgro Ethics Hotline

This Policy has been designed to comply with the provisions of the Protected Disclosures Act 26 of 2000 and Protected Disclosures Amendment Act 5 of 2017.

Any suspicion of fraud and corruption will be treated seriously and will be reviewed, analysed, and if warranted, investigated. If an employee becomes aware of a suspected fraud, corruption or any irregularity or unethical behaviour, such issues should be reported in terms of the Code of Ethics Policy. This policy should not be abused, for the pursuit of other agendas and Remgro reserves the right to initiate civil and/or criminal action against such an individual.

8.2 Investigating fraud and corruption

Dealing with suspected fraud and corruption

In the event that fraud or corruption is detected or suspected, investigations will be initiated, and if warranted, disciplinary proceedings, prosecution or recovery action will be initiated.

Investigations

Any reports of incidents of fraud and/or corruption will be confirmed by thorough and independent investigation. Anonymous reports may warrant a preliminary investigation before any decision to implement an independent investigation is taken.

Investigations will be undertaken by appropriately qualified and experienced persons who are independent of the section/unit where investigations are required. Independence and objectivity of investigations are paramount and the scope and objective of the investigation will be contained in an investigation mandate.

Investigations will be mandated by the Chief Executive Officer, Chief Financial Officer, in conjunction with the Chief Audit Executive and reported to the Chairman of the Audit and Risk Committee.

Disciplinary proceedings

The ultimate outcome of disciplinary proceedings may involve a person/s receiving written warnings or the termination of their services. All disciplinary proceedings will take place in accordance with the procedures as set out in the disciplinary procedures.

Prosecution

Should investigations uncover evidence of fraud or corruption in respect of an allegation or series of allegations, executive management will review the facts at hand to determine whether the matter is one that ought to be reported to the relevant law enforcement agency for investigation and possible prosecution. The company will give its full co-operation to any such law enforcement agency including the provision of reports compiled in respect of investigations conducted. Where required by law, instances of suspected irregularities will be disclosed to the required law enforcement agencies.

Recovery action

Where there is clear evidence of fraud or corruption and there has been a financial loss to the company, recovery action, criminal, civil or administrative, will be instituted to recover any such losses. In respect of civil recoveries, costs involved will be determined to ensure that the cost of recovery is financially beneficial.

Internal control review after discovery of fraud

The responsibility for ensuring that the internal control environment is re-assessed and for ensuring that the recommendations arising out of this assessment are implemented is that of Line Management of the Department(s) concerned.

The Chief Audit Executive will maintain a register of fraud and related incidents for reporting to the Audit and Risk Committee, including written confirmation of all Ethics Hotline calls received.

9. BEST DEFENCE STRATEGY

As mentioned in 2.1.6 above, Section 7(2) of United Kingdom's Bribery Act, an organisation has a defense if it can prove that, while bribery did take place, it had in place "adequate procedures designed to prevent persons associated with the organisation from undertaking such conduct". Under the Act's explanatory notes, the burden of proof in this situation is on the organisation, with the standard of proof being "on the balance of probabilities".

As such Remgro will implement and maintain as part of its Risk Management processes and Ethics policies the following procedures aimed at demonstrating that a best defense strategy is in place:

Due Diligence

Prior to making recommendations to any Committee delegated to approve potential investments, the Investment Division will ensure that adequate risk assessment and due diligence was done to ensure that the target did not obtain any of its business licenses, key contracts, or related assets by means of any fraudulent or corrupt practice, either directly or indirectly. Contracts will also ensure that the required warranties are obtained in these instances. Where such instances may be detected or the required assurances could not be obtained the impacts and implications thereof must be adequately disclosed and valuations must be aligned with the commercial consequences of immediate termination of such practices, contracts or assets post investment. In addition, contracts must secure the implementation and compliance with best practice as regards ethical governance.

The above due diligences will be extended to directors, shareholders and key officers of any target company.

Where agents or intermediaries are being implemented as part of a marketing, procurement or investment structures the above due diligence process will be extended to such parties prior to finalising such envisaged contracts, which contracts will also require compliance to ethical conduct and best practice standards.

Awareness

Continuous awareness initiatives ensure that all employees are aware of the ethical and compliance requirements of this Policy and related legislation.

Monitoring and review

Compliance with this Policy is tested as part of the internal audit process.

This policy was approved by the Risk, Opportunities, Technology and Information Governance Committee on 15 February 2023.

1 REGULATORY FRAMEWORK

1.1 Summary of statutory offences relating to dishonesty

1.1.1 Prevention and Combating of Corrupt Activities Act 12 of 2004 (PRECCA)

The Prevention and Combating of Corrupt Activities Act (generally referred to as "PRECCA") is aimed at the strengthening of measures to prevent and combat corrupt activities.

The offence defined by the Act relates to the giving or receiving of a ***"gratification"***. The term ***gratification*** is defined in the Act and includes a wide variety of tangible and intangible benefits such as money, gifts, status, employment, release of obligations, granting of rights or privileges and the granting of any valuable consideration such as discounts, etc.

As far as offences are concerned, the Act defines a general offence of corruption. In addition to the general offence, certain specific offences are defined relating to specific persons or specific corrupt activities.

The general offence of corruption is contained in Part 1 (section 3) of the Act. This section provides that any person who gives or accepts or agrees or offers to accept/receive any gratification from another person in order to influence such other person in a manner that amounts to:

- The illegal or unauthorised performance of such other person's powers, duties or functions;
- An abuse of authority, a breach of trust, or the violation of a legal duty or a set of rules;
- The achievement of an unjustified result; or

Any other unauthorised or improper inducement to do or not to do anything is guilty of the offence of Corruption.

Section 34 of the Act places a duty on *any person* who holds a position of authority and who knows or ought reasonably to have known or suspected that any other person has committed certain corrupt or illegal activities, to report the same to a police official. These include certain offences of corruption created under the Act as well as fraud, theft, extortion and forgery where the amount involved is R100 000 or more. Failure to report such suspicion constitutes an offence. Persons who hold position of authority is widely defined in the Act.

Offences under the Act are subject to penalties including a maximum imprisonment for life or fines of up to R250 000. In addition to any fine, a court may impose a fine equal to five times the value of the gratification involved in the offence.

Section 17 of the Act provides that a public officer who acquires or holds a private interest in any contract, agreement or investment connected with the public body in which he/she is employed, is guilty of an offence unless:

- The interest consists of shareholding in a listed company;
- The public officer's conditions of employment do not prohibit him/her from acquiring such interests; or
- In the case of a tender process, the said officer's conditions of employment do not prohibit him/her from acquiring such interests as long as the interests are acquired through an independent tender process.

1.1.2 Prevention of Organised Crime Act, 121 of 1998 (POCA)

The Prevention of Organised Crime Act, as amended, (generally referred to as "POCA") contains provisions that are aimed at achieving the following objectives:

- The combating of organised crime, money laundering and criminal gang activities;
- The criminalisation of conduct referred to as "racketeering";

- The provision of mechanisms for the confiscation and forfeiture of the proceeds of crime;
- The creation of mechanisms for the National Director of Public Prosecutions to obtain certain information required for purposes of an investigation; and
- The creation of mechanisms for co-operation between investigators and the South African Revenue Services (SARS).

Section 4 of the Act defines the "general" offence of money laundering and provides that a person who knows, or ought reasonably to have known that property is or forms part of the proceeds of unlawful activities, commits an act in connection with that property which has the effect (or is likely to have the effect) of concealing the nature or source thereof; or enabling any person who has committed (or commits) an offence to avoid prosecution or to remove/diminish the property, shall be guilty of an offence.

Section 5 of the Act creates an offence if a person knows or ought reasonably to have known that another person has obtained the proceeds of unlawful activities and provides assistance to such other person regarding the use or retention of such property.

Section 6 of the Act creates an offence if a person knows or ought reasonably to have known that property is or forms part of the proceeds of unlawful activities and acquires uses or possesses such property.

The above offences are regarded as very serious and the Act contains exceptionally harsh penalties relating to these offences. A person convicted of one of the above offences is liable to a maximum fine of R1000 million or to imprisonment for life. Prescribed penalty by law for perjury.

1.1.3 Financial Intelligence Centre Act, 38 of 2001 (FICA) and Financial Intelligence Centre Amendment Act, 1 of 2017

The Financial Intelligence Centre Act ("FICA") came fully into force on 1 February 2002. During April 2017, the President assented the Financial Intelligence Centre Amendment Act ("Amendment Act"). Just as FICA, its various sections will come into operation overtime.

The Financial Intelligence Centre Amendment Act amends the Financial Intelligence Centre Act, 2001 which aims to fight financial crimes, such as money laundering, tax evasion and terrorist financing activities.

The key amendment introduced, is a shift from a rules-based approach to a risk-based approach in ensuring FICA compliance, which simply means that accountable institutions must consider the potential risk involved with establishing a business relationship or concluding a single transaction with a particular client.

Accountable institutions are obliged to conduct "client due diligence" ("CDD") to establish and verify the identities of their clients. Essentially you are required to know who your client is with whom you are doing business. The Amendment Act now imposes enhanced measures relating to ongoing CDD and the monitoring of business relationships, as well as obligations in respect of prominent and influential persons.

The Act imposes compliance obligations on so-called "accountable institutions" which are defined in Schedule 1 to the Act. These include:

- An obligation to keep due diligence records;
- An obligation to retain records of all business transactions;
- A duty to report certain transactions;
- An obligation that their employees receive comprehensive and ongoing training on FICA in accordance with their Risk Management and Compliance Programme to ensure that employees are aware of their duties in terms of FICA when engaging with clients.

Accountable institutions are obliged to develop, document, implement and maintain a Risk Management and Compliance Programme, which sets out the FICA compliance obligations of the business and its procedures for ensuring that these obligations are met. The Amendment Act dictates that the Risk Management and Compliance Programme replaces the formerly required FICA internal rules of the organisation.

Regarding the reporting of suspicious transactions, FICA makes provision for a duty to report “suspicious or unusual transactions”. In this regard, it provides that any person who carries on a business or is in charge of or manages a business or is employed by a business and who knows or suspects certain facts has a duty to report their knowledge or suspicion to the FIC within a prescribed period. Matters that require reporting include knowledge or suspicion of the following:

- The receipt of proceeds of unlawful activities;
- Transactions which are likely to facilitate the transfer of proceeds of unlawful activities;
- Transactions conducted to avoid giving rise to a reporting duty under FICA;
- Transactions that have no apparent business or lawful purpose;
- Transactions relevant to the investigation of tax evasion; or
- The use of a business entity for money laundering purposes.

The Amendment Act changed certain types of conduct, currently criminalised in FICA, to acts of non-compliance, which are punishable through administrative sanctions. Non-compliance with provisions, directives and regulations issued by the Financial Intelligence Centre relating to administrative sanctions now carries a maximum financial penalty not exceeding R10 million in respect of a natural person and R50 million in respect of any legal person.

However, a person convicted of an offence mentioned in sec 55, 61A, 62A, 62B, 62C, 62D is liable to imprisonment for a period not exceeding 15 years or to a fine not exceeding R100 million (per contravention).

1.1.4 Protection of Constitutional Democracy Against Terrorist and Related Activities Act 33 of 2004 ("POCDATARA")

On May 20, 2005, the Protection of Constitutional Democracy Against Terrorist and Related Activities Act (“POCDATARA”) came into effect criminalising terrorist activity and terrorist financing and gave the government investigative and asset seizure powers in cases of suspected terrorist activity.

POCDATARA provides for two new reporting obligations under section 28A and section 29 of FICA. The Money Laundering Control Regulations under FICA have also been amended, with effect from 20 May 2005, for this purpose. The amended regulations now provide for detailed reporting related to terrorist financing, under new sections 28A and 29 of FICA.

The POCDATARA amends section 29 of FICA to extend the reporting of suspicious and unusual transactions to cover transactions relating to "property which is connected to an offence relating to the financing of terrorist and related activities" or to "the financing of terrorist and related activities". The POCDATARA introduces a new section 28A of FICA that requires the reporting of any property that is associated with terrorist and related activities to the FIC.

Non-compliance is regarded as very serious and the Act contains exceptionally harsh penalties relating to same. A person convicted of one of non-compliance is liable to a maximum fine of R100 million or to imprisonment for life.

1.1.5 Companies Act 71 of 2008

Various sanctions against directors who:

- Fail to act in the best interest of the company and/or
- Fail to protect the company’s assets
- Have conflicts of interest

There are various other possible transgressions listed in the Companies Act, such as failure to keep proper accounting records, and this list is therefore not deemed exhaustive.

The Companies and Intellectual Property Commission ("CIPC") has published a compliance checklist to ensure compliance of the mandatory requirements of the Companies Act, 2008. The compliance checklist serves as an educational tool for directors and company secretaries, in guiding them with regards to their responsibilities in terms of the Act. The CIPC will utilise the checklist to monitor and regulate proper compliance with the Act.

Non-compliance of the Act carries a financial penalty (not specified). Provisions of Adjustment of Fines Act 101 of 1991 applies to calculate penalty. In addition to a fine, a court may impose imprisonment for a period of up to 10 years. The CIPC may remove a company from the companies register and a director of a company is liable for any loss, damages or costs sustained by the company as a direct or indirect consequence of the director having acted in the name of the company, signed anything on behalf of the company, or purported to bind the company or authorise the taking of any action by or on behalf of the company, despite knowing that the director lacked the authority to do so.

1.1.6 International Legislation and convention

Where the company operates outside the boarder of South Africa and/or holds international interest, this policy will extend to also include other relevant international legislation where these are more onerous. The following serve as examples:

- United Nations Convention against Corrupt Activities
- Bribery Act, 2010 (United Kingdom)
- Foreign Corrupt Practices Act (FCPA) (United States of America)
- African Union Convention on Preventing and Combatting Corruption
- OECD Convention on Combatting Bribery of Foreign Public Officials in International Business Transactions (OECD Anti-Bribery Convention)

The United Nations Convention against Corruption is the only legally binding universal anti-corruption instrument. The Convention's far-reaching approach and the mandatory character of many of its provisions make it a unique tool for developing a comprehensive response to a global problem. The Convention covers five main areas: preventive measures, criminalization and law enforcement, international cooperation, asset recovery, and technical assistance and information exchange. The Convention covers many different forms of corruption, such as bribery, trading in influence, abuse of functions, and various acts of corruption in the private sector. A highlight of the Convention is the inclusion of a specific chapter on asset recovery, aimed at returning assets to their rightful owners, including countries from which they had been taken illicitly. The vast majority of United Nations Member States are parties to the Convention.

In the United Kingdom the Bribery Act 2010 provides for a general offense of bribery, which criminalises both the receipt and payment of bribes. According to this Act a bribe is paid where a person receives, offers or gives a bribe intending that, as a consequence, a function should be performed "improperly".

The Bribery Act provides three examples of when a function would be deemed to have been carried out "improperly":

(a) The person performing it is expected to perform the function or activity in good faith, but does not.

(b) The person performing it is expected to perform it impartially, but does not.

(c) The person is in a position of trust, but breaches that trust.

The types of functions that are covered by the Bribery Act are as follows:

(a) Functions of a public nature

(b) Activities connected with a business

(c) Activities performed in the course of a person's employment

(d) An activity performed by or on behalf of a body of persons

A corporate or commercial organisation will also commit an offence under Section 7 of the Bribery Act, where a person "associated with" it bribes another person, intending to obtain or retain business for the organisation or to obtain or retain an advantage in the conduct of business for the organisation. This is a strict liability offense.

Note the following:

(a) A person will be "associated with" the company for these purposes, where the person acts on an organisation's behalf. This could include an employee, agent or subsidiary of the organisation. Contractors, suppliers, joint venture entities and joint venture partners may also be associated persons.

(b) While there is a rebuttable presumption that an employee acts on behalf of his or her organisation, an individual's association will be determined by reference to all relevant circumstances, not merely the relationship between the individual and the organisation.

(c) It is a defence for an organisation to prove that it had "adequate procedures" in place to prevent the bribery.

An individual convicted of committing any of the general bribery offenses may be imprisoned for a term of up to 10 years; and/or receive an unlimited fine.

A company or partnership that commits any of the general bribery offenses will be liable on conviction on indictment, to an unlimited fine, and the automatic and perpetual debarment from competing for public contracts.

A conviction under Section 7 of the Bribery Act will attract discretionary rather than mandatory disbarment from competing for public contracts. Where an organisation has been convicted of a bribery offense, senior officers of the organisation who have consented to or connived in the conduct can also be convicted of the offense concerned.

The Foreign Corrupt Practices Act (FCPA) is a United States law passed in 1977 that prohibits U.S. firms and individuals from paying bribes to foreign officials in furtherance of a business deal. The FCPA places no minimum amount for a punishment of a bribery payment.

The African Union (AU) Convention on Preventing and Combating Corruption, adopted in 2003, addresses corruption in the public and private sectors. It represents a consensus on what African countries should do in the areas of prevention, criminalisation, international cooperation and asset recovery.

The OECD Anti-Bribery Convention is an anti-corruption convention of the OECD aimed at reducing political corruption and corporate crime in developing countries, by encouraging sanctions against bribery in international business transactions carried out by companies based in the Convention member countries.

1.2 Statutes combating fraud and corruption

1.2.1 Protected Disclosures Act 26 of 2000 (As amended by the Protected Disclosures Amendment Act 5 of 2017)

The Protected Disclosures Act is designed to encourage a culture of whistle-blowing in the workplace and is commonly referred to as the "Whistle-blowers Act". The objects of the Act are to protect an employee from being subjected to an occupational detriment on account of having made a protected disclosure and to provide for procedures in terms of which any employee can disclose information regarding improprieties by his/her employer, in a responsible manner.

The Act prohibits the employer from:

- Dismissing, suspending, demoting, harassing or intimidating the employee;
- Subjecting the employee to disciplinary action;
- Transferring the employee against his or her will;
- Refusing due transfer or promotion;
- Altering the employment conditions of the employee unilaterally;
- Refusing the employee a reference or providing him/her with an adverse reference;

- Denying appointment;
- Threatening the employee with any of the above activities; or
- Otherwise adversely affecting the employee in respect of his/her employment, profession or office, including employment opportunities and work security, if the disclosure is made in terms of the Act.

An employee who is dismissed for making a protected disclosure can claim either compensation, up to a maximum of 2 years' salary, or reinstatement.

However, when abused, the Act, does not provide whistle-blowers with blanket immunity from civil and criminal liability.

There are furthermore many international laws and conventions, which may be of relevance in other countries where business is conducted and these should be taken cognisance off if operating in such jurisdictions.