FRAUD AND CORRUPTION PLAN

Current at October 2021

Version Control

Last Review Date	Version	Status	Owned & Issued By	Comments
15/12/16	1.0	Final	Chief Risk Officer	Initial development
19/05/2020	1.1	Draft	Fraud Risk Manager	This revision was to: • Conduct a regular review of the control plan and to complete the observation included in the recent PwC Fraud Management Review; • Include the roles & responsibilities of the Fraud Risk Manager; • Document the roles & responsibilities for fraud controls; • Review and amend the Internal Investigations section; • Include Fraud Losses; and • Name change for Human Resources to People & Performance and Support Services Operations
27/05/2020	2.0	Final	Chief Risk Officer	Approved
12/10/2021	2.1	Review	Fraud Risk Manager	Revision to include Corporate Governance recommendations and update branding
19/10/2021		Final	Chief Risk Officer	Approved

Distribution

Title	Sign Off/Review
Chief Risk Officer	Owner/ Sign Off
Chief Customer Officer	Sign-Off
Chief People & Property Officer	Sign-Off
Chief Information Officer	Sign Off
Chief Operating Officer	Sign Off
Chief Financial Officer	Sign Off

Table of Contents

1 INTRODUCTION

Auswide Bank is committed to preventing and controlling fraud and corruption against it, whether internally or externally.

The Fraud and Corruption Plan has been developed as a framework to give all stakeholders guidance and direction on the processes for preventing, detecting and responding to fraud and corruption within Auswide Bank.

This Plan will be periodically reviewed to check that it is operating effectively and to make amendments as required.

2 PURPOSE

This Framework aims to:

- build a culture within Auswide Bank that seeks to prevent fraud and corruption;
- reduce the potential for fraud and corruption within and against Auswide Bank; and
- explain how Auswide Bank will use risk management practices to prevent and control fraud and corruption; and provide guidance on how any suspected instances of fraud and corruption within the organisation will be dealt with by Auswide Bank.

3 DEFINITIONS

- **Contractor**
  A person other than an Auswide Bank employee who provides professional or non-professional services to Auswide Bank (e.g. cleaning, trades people, or expert consultancy services).
- **Corruption**
  Dishonest activity or inactivity in which an Auswide employee acts contrary to the interests of Auswide Bank in order to achieve some gain or advantage, or to avoid loss or disadvantage, for the employee or for another person or entity. Corruption can include, but is not limited to, behaviour such as fraud, deception or misuse of a position or authority.
- **Fraud**
  A dishonest activity causing actual or potential financial loss to any person or entity including theft of monies or other property by employees or persons external to the entity and whether or not deception is used at the time, immediately before or immediately following the activity. This also includes the deliberate falsification, concealment, destruction or use of falsified documentation used or intended for use for a normal business purpose or the improper use of information or position for personal financial benefit.
- **Fraud risk**
  The risk of loss from internal fraud or external fraud. These can be defined as:
  a) **Internal fraud** - losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy (excluding diversity / discrimination events) which involves at least one internal party (employee, contractor or agent); or
  b) **External fraud** – losses due to acts of a third party that are of a type intended to defraud, misappropriate property or circumvent the law by a third party. Examples of external fraud may include-

- Fraud perpetrated against a customer – a false and erroneous representation by a fraudster that they were acting on behalf of Auswide Bank to perpetrate a fraud against an Auswide Bank customer or other party.
- Fraud perpetrated against Auswide Bank – may be a fraudulent email sent as though it was from an Auswide Bank customer to Auswide Bank for the purpose of perpetrating fraud against either Auswide Bank or our customer

Refer to Appendix 1 Examples of common types of fraud and acts of corruption.

4 FRAUD AND CORRUPTION PREVENTION

A major reason people commit fraud or acts of corruption is because they can. The threat of fraud or corruption can come from inside or outside the organisation, but the likelihood is greatly decreased when a comprehensive system of control is established, which aims to prevent fraud and corruption, and where fraud and corruption is not prevented, increases the likelihood of detection and increases the cost to the fraudster or person committing the act of corruption.

4.1 Why do People Commit Fraud and Corruption?

Fraud and corruption is likely to result from a combination of three factors: motivation, opportunity and rationalisation.

- **Motivation**
  In simple terms, motivation is typically based on either greed or need.
- **Opportunity**
  Fraud and corruption is more likely in organisations where there is a weak internal control system, poor security over company property, little fear of exposure and likelihood of detection, unclear policies with regard to acceptable behaviour and a perception that there are no consequences for their behaviour.
- **Rationalisation**
  Some people may be able to rationalise fraudulent and corrupt actions as:
  • necessary
  • harmless
  • justified

One of the most effective ways to deal with the problem of fraud and corruption is to adopt methods that will decrease motive, restrict opportunity and limit the ability for potential offenders to rationalise their actions. In the case of deliberate acts of fraud and corruption, the aim of preventative controls is to reduce opportunity and remove temptation from potential offenders. Prevention techniques include the introduction of policies, procedures and controls, and activities such as training and fraud awareness to stop fraud from occurring.

4.2 Developing a Sound Ethical Culture

Attitudes within an organisation often lay the foundation for a high or low fraud risk environment. Where minor unethical practices may be overlooked (e.g. petty theft, expense frauds), larger frauds committed by higher levels of management may also be treated in a similar lenient fashion. In this

environment there may be a risk of total collapse of the organisation either through a single catastrophic fraud or through the combined weight of many smaller frauds.

Organisations which have taken the time to consider where they stand on ethical issues have come to realise that high ethical standards bring long term benefits as customers, suppliers, employees and the community realise that they are dealing with a trustworthy organisation. They have also realised that dubious ethical or fraudulent practices cause serious adverse consequences to the people and organisations concerned when exposed. To foster a strong organisational culture that will help to protect against fraud and corruption, Auswide Bank will:

- raise awareness of ethical behaviours by implementing initiatives to deter and minimise the opportunities for fraud and corruption;
- promote Auswide Bank's values and ethical conduct in the Code of Conduct;
- provide training to promote awareness of Auswide Bank's expectations regarding fraud and corruption control
- prohibit bribes or improper payments to public officials and have controls around political donations; and
- prohibit any secret commission payments

4.2.1 Auswide Risk Culture Statement

We understand that risk is everyone's responsibility. We manage risk in a sustainable way by balancing risk and reward to mitigate potential loss or reputational damage and maximise growth opportunities.

4.2.2 Training

Auswide Bank utilises the e3Learning platform to deliver a range of training courses for its employees. The 'Fraud and Corruption Awareness and Prevention' training course draws on the content of the 'Australian Standard 8001-2008 Fraud and Corruption Control', and covers a range of topics including –

- Fraud and corruption
- Fraud and corruption prevention and ethical behaviour
- Reporting fraud and corruption

It is compulsory for all Auswide Bank employees to complete the Fraud and Corruption Awareness and Prevention training annually.

The 'Introduction to Risk Management' training course is completed by all leaders in the Bank at induction and covers the following topics:

- Nature and Types of Risk
- Risk Management, Framework & Standards
- Risk Management Process

4.3 Internal Control Systems

Key aspects of preventing fraud include ensuring internal controls are in place to manage potential fraud risks, identifying control weaknesses and implementing measures to address these weaknesses. Regular fraud risk assessments are vital in identifying potential risks and control weaknesses and appropriate treatments.

Section 2 of the Auswide Risk Management Strategy provides guidance on how Auswide Bank's Risk and Compliance System known as TriLine GRC, is used to manage the complete lifecycle of a risk from identification, assessment, treatment and review; track operational risks across Auswide Bank and enables Risk Owners to take responsibility.

Risk and Control Assessments (RCAs) should encompass all material business processes to help identify material risks identified including fraud risk and evaluate the key controls which:

- Prevent the risk from materialising
- Detect a risk event if it occurs
- Minimise the impact of the risk event

An internal control system comprises all those policies and procedures that, taken together, support an organisation's effective and efficient operation. Internal controls typically deal with factors such as approval and authorisation processes, access restrictions and transaction controls, account reconciliations, and physical security. These procedures often include the division of responsibilities and checks and balances to reduce risk. To help address fraud and corruption, Auswide Bank will:

- maintain a Conflict of Interest Register;
- maintain the Board Audit and Board Risk Committees;
- consider fraud and corruption risks in developing the Risk Register;
- ensure financial transactions are properly authorised and processed;
- develop and implement policies and procedures that identify and address fraud risks within work processes, and make these available to all Auswide Bank employees; and
- monitor the effectiveness of internal control structures, and report instances where the internal control appears not to be working as it was designed to.

Auswide Bank acknowledges that while it is worth investing in fraud and corruption prevention techniques, it alone cannot provide 100% protection, as it is difficult, if not impossible, to remove all avenues of opportunity for perpetrating fraud and corruption.

4.3.1 Policies, Procedures and Related Documents

- Auswide Banking Services Manual
- Promapp Procedures
- Broker Accreditation Process Manual
- Business Banking Lending Policy
- Code of Conduct for Directors & Key Executives
- Conflicts of Interest Policy
- Consumer Credit Policy
- Contract Management Manual
- Auswide Bank Code of Conduct & Ethics
- Whistleblower Protection Policy Reporting Procedure
- Human Resources Manual Section 5 - Grievance, Discipline, Misconduct, Absence and Poor Performance Policy, and Section 2.12 Recruitment Policy
- Incident Reporting and Management Procedures Manual

- Information Technology Principles & Governance Manual
- Information Technology Security and Standards Manual
- Information Security User Manual
- Outsourcing Risk Management Manual
- Risk Management Strategy AB206
- Risk Appetite Statement

4.4 Screening

4.4.1 Employee Screening

To help reduce the risk of employee fraud and corruption, Auswide Bank has developed a Recruitment Policy and a Conflicts of Interest Policy that requires:

- Police , Bankruptcy, ASIC banned officers and previous employment checks are conducted on new employees/key executives;
- AML Employee Due Diligence checks performed on a risk based approach at regular intervals; and
- Annual reminders to be sent to all Auswide Bank employees regarding the declaration of conflicts of interest and the maintenance of a register of declared interests.

4.4.2 Supplier/Contractor Screening

To help reduce the risk of fraud and corruption in its procurement and contracting processes, Auswide Bank has developed a Contract Management Manual that requires:

- where appropriate, the selection of service providers to be conducted by a tender process; and
- a comprehensive due diligence process to be undertaken where the contract is assessed as a material business activities pursuant to APRA Prudential Standard CPS 231 – Outsourcing

A register of all contractors is also maintained within the Contracts Module of TriLine GRC.

5 FRAUD AND CORRUPTION DETECTION

To help detect suspected fraud and corruption within the Bank, Auswide Bank will:

- promote a culture of reporting through induction, training, policies and procedures;
- ensure fraud risk is incorporated within the Internal Audit plan;
- monitor Auswide Bank employee adherence to information security and information technology policies and procedures; and
- as required, engage external and internal auditors to:
    - perform financial data analytics on the traditional high-risk finance areas; or/and
    - conduct regular and automated post-transactional monitoring of identified high-risk processes (e.g. payroll analytics and finance system analytics)

5.1 Identification of Early Warning Signs (Red Flags)

Identifying and acting on warning signs (red flags) is paramount to the early detection of fraud and corruption.

Red flags do not indicate guilt or innocence, but they provide warning signs of possible fraud. There are two types of red flags:

- Behavioural; and
- Transactional.

Behavioural red flags refer to unusual actions behaviours or traits exhibited by a person. Some examples are provided in the table below.

Transactional red flags refer to unusual or out of the ordinary exchanges related to common business activities or transactions.

5.1.1 Early Warning Signs (Red Flags)

Transactional Red Flags
• Transactions occurring at an unusual time (of day, week, month, year or season); • Frequency of the transaction is unusual (too many or few); • Place of transaction is unusual; • Amount of the transaction is unusual (too high, too low, too alike, too different); or • Unusual relationships between persons (related parties, perceived strange relationship between parties, management performing clerical functions).
Behavioural Red Flags
• Employee lifestyle changes: expensive cars, jewellery, homes, clothes; • Employee exorbitant/excessive lifestyle, personal circumstances or purchases not matched with income (e.g. significant gambling addiction may increase the likelihood of committing fraud); • Creditors or collectors appearing at the workplace; • Employees refusing vacations, sick leave or promotions – may have a fear of detection; • Lack of a strong code of personal ethics; • A strong desire to beat the system; • Employee criminal history; • Employees persistent and/or unnecessary taking control of records; • Employees insisting on working unusual or non-standard business hours; or • Employees avoiding or delaying provision of documentation when requested by Auditors.

6 RESPONDING TO FRAUD AND CORRUPTION

6.1 Roles and Responsibilities

Business Unit Manager and Supervisor

Each business unit is responsible for managing the outcome of fraud and corruption risk related activities under a “Three Lines of Defence” model. This includes the development, implementation and review of their fraud controls and their recording in TriLine.

Generally, managers and supervisors are in a position to take responsibility for detecting fraud and other irregularities in their area. Employees must assist management by reporting any suspected irregularities.

All Employees

All employees have a responsibility to report any suspicions of fraud.

Normally it is expected that employees should raise their concerns with their Reporting Manager. However, if the actual employee’s report involves their Reporting Manager, or they think that it may be inappropriate to disclose the information directly to their Reporting Manager for any reason, then

employees should raise their concerns with the Fraud Risk Manager, The Chief Risk Officer, the Chief People & Property Officer or a Senior Executive Manager at Head Office, as specified in the Whistleblower Protection Policy Reporting Procedure. Any disclosure under the Whistleblower Protection Policy will be treated as completely confidential and will not result in any report to anyone within our organisation, unless the employee agrees to the contrary, or it is required by law.

Employees may raise any concerns under the procedure anonymously, in writing, to the appropriate person. However, if the employee remains anonymous, then this may hamper our ability to investigate their concerns.

Auswide Bank will try to investigate the matter employees have raised as soon as is reasonably practicable. Employees may be requested to put their concerns in writing or to attend as a witness during any stage of the investigation. If employees are requested to attend, then employees will normally be permitted to be accompanied by an appropriate support person.

If employees are unhappy about the speed of the investigation or the way in which the matter has been investigated or resolved, then employees should confirm their concerns in writing.

If employees believe they are being subjected to a detriment by any person within Auswide Bank organisation as a result of them raising concerns under this procedure, then employees must immediately inform the Chief Risk Officer, or the Chief People & Property Officer. Auswide Bank will then take appropriate action.

Chief Risk Officer

The Chief Risk Officer will have responsibility for initiating and overseeing:

- all fraud investigations
- implementing the fraud response plan
- any follow-up actions

Chief Risk Officer is independent from business lines, other revenue-generating responsibilities and is responsible for monitoring potential risks applicable to Auswide Bank and is the liaison with APRA. The Chief Risk Officer has a direct reporting line to the Managing Director, and has regular and unfettered access to the Board and the Board Risk Committee.

Fraud Risk Manager

The Fraud Risk Manager has responsibility for:

- Oversight and assist with the review and development of Auswide's Fraud Risk Management and supporting framework;
- Assist with creating and promoting a culture of risk awareness;
- Administer, monitor and report on Auswide's Fraud Risk Profile and key risk indicators;
- Be the main contact point for Auswide across fraud forums;
- Engage and consult with relevant areas of the Bank to develop action plans that effectively manage identified Fraud risk and ensure they are captured in business requirements;

- Extract and provide analytical comment and develop fraud scenarios relevant to Auswide's product and processes;
- Provide second line of defence by undertaking test reviews of Auswide's Internal Fraud Risk Controls to ensure business units are adequately managing Fraud Risk;
- Advise on potential fraud risks/impacts; and
- Undertake fraud investigations in line with Risk and compliance requirements, along with documenting them accordingly.

Chief People & Property Officer

The Chief People & Property Officer has the responsibility for any internal disciplinary policies and procedures.

Advice should be sought in relation to the employee management strategies, individually employment histories, and issues relating to employment law or equal opportunities.

Board Audit Committee

The Board Audit Committee will have responsibility for:

- overviewing Auswide Banks internal control including the design and implementation of anti-fraud controls
- integrity of the financial statements;
- review reports from the Internal Auditor, the Internal Audit program and any Management responses to issues raised in relation to Fraud prevention

Board Risk Committee

The Board Risk Committee will have responsibility for:

- assisting Board to set and oversee the Fraud risk profile and fraud risk management framework
- ensuring appropriate Fraud risk systems and practices to effectively operate within Board approved risk profile

Appointed Auditor

The Appointed Auditor will have responsibility for:

- providing an independent and objective view on the truth and fairness of financial statements.
- making an assessment of the systems, procedures and controls used to address compliance with prudential requirements and for the purposes of producing reliable financial data. The Appointed Auditor may also be required to perform other work as necessary to fulfil their responsibilities under APS 310

Internal Audit

The Internal Auditor will have responsibility for:

- assessing the adequacy of the control framework as a key element of individual audit plans
- providing independent review obligations per CPS220 as to the effectiveness of, the risk management framework at least annually.

- in addition, the appropriateness, effectiveness and adequacy of Auswide Bank's risk management framework must be comprehensively reviewed at least every three years.
- reporting results and findings to the Board Audit Committee.

6.2 Internal Investigations

The Chief Risk Officer will be responsible for managing investigations either internally or by appointing an external party where appropriate. Each case will be treated according to the particular circumstances and professional advice will be sought where necessary. Where there are reasonable grounds for suspicion, the police will be involved at an early stage.

There may be cases, where police may be on site pending the completion of the interview, or the police may be the first people to speak with the employee.

Interviewing employee(s)

If the Chief Risk Officer agrees to proceed with interviewing an employee, and where the suspect is an employee of Auswide Bank, the interview will be carried out by the investigator and the manager-once-removed. Consultation with the Chief People & Property Officer is mandatory throughout the process. The individual(s) being interviewed should be informed 24 hours in advance in writing of the reason for the interview and contained within the letter is that the meeting will be digitally recorded. The individual(s) being interviewed will be given the opportunity to have an independent support person – can be a friend or union official.

The investigator will determine if the interview requires suspension at any time and will consult with the Chief Risk Officer and Chief People & Property Officer and will determine the appropriate time for police advice to be sought.

Where external organisations/individuals are involved, interviews will generally be undertaken by the police unless the Chief Risk Officer is able to gain the co-operation of the organisation's management or auditors.

Witness statements

If a witness is prepared to give a written statement the staff member will draft the statement in conjunction with the investigator in the witness's own words. The witness will be asked to sign the document as a true record.

Should a staff member be requested to provide a formal witness statement, they are to attend their local police station and do so. The staff member can refer to the Fraud Risk Manager for assistance with this.

Physical and electronic evidence

The investigator and Chief Risk Office will take control of any physical evidence and maintain a record of where, when and from whom it was taken. Where the evidence consists of several items these will be tagged with a reference number which corresponds with the written record of the investigation, ensuring that electronic evidence is appropriately handled.

6.3 Disciplinary procedures

Zero tolerance means that certain actions will not be tolerated under any circumstances with breaches treated with the utmost seriousness. Auswide Bank has determined it has zero tolerance for employees committing internal fraud. To ensure substantiated incidents of fraud are dealt with appropriately, Auswide Bank will take appropriate disciplinary action as specified in the Human Resources Manual Section 5 - Grievance, Discipline, Misconduct, Absence and Poor Performance Policy All instances of fraud or attempted fraud, will be referred by the investigator to the police.

6.4 Insurance

To mitigate the effects of fraud on Auswide Bank's resources, Auswide Bank will:

- Maintain an appropriate policy to cover fraud and associated costs
- Ensure all service providers engaged by Auswide Bank hold appropriate professional indemnity insurance

6.5 Review Process

To continuously improve its ability to prevent and deal with fraud and corruption Auswide Bank will:

- use the Internal Audit function to review processes and provide recommendations for improved systems;
- respond promptly to audit findings and recommendations;
- report all incidents of alleged or proven fraud or corruption to the Managing Director, Chief Risk Officer and Internal Audit function;
- record all incidents of proven fraud or corruption in the TriLine GRC Incident Register;
- use risk incidents and risk reporting profiles to identify risks, review the Strategic Risk Profile, identify risk mitigation strategies and report to relevant managers and the Board Audit and Board Risk Committees;
- take risk incidents reported in the TriLine Incident Register into account when developing the Internal Audit Plan;
- support and implement investigation outcomes and subsequent recommendations
- take appropriate actions in regard to recommendations;
- review policies and procedures, taking into account recent risk incidents and recommendations by the Internal Audit function; and
- reinforce Auswide Bank employee awareness of internal controls and prevention mechanisms through training on any new processes or procedures.

The Fraud Risk Manager will review annually the Fraud & Corruption Control Plan and amend where necessary with approval from the Chief Risk Officer. The review will be recorded in TriLine, regardless of whether updates are made or not.

6.6 Fraud Losses

When a fraud loss occurs at Auswide, the loss amount will be debited to the applicable Fraud Loss General Ledger. The transaction will occur based off the recommendations contained within the completed fraud report. To ensure segregation of duties, whilst a refund will be recommended and approved by the Chief Risk Office, the processing will be completed by Support Services Operations.

Fraud losses will be subject to the below delegations:

Card Fraud	As per delegations currently operated by Support Services
	Losses >$2K (or systemic issues/organised crime) details provided by email to fraud@auswidebank.com.au
All other fraud	Losses <$5,000 approved by Fraud Risk Manager
	Losses <$250,000 approved by Chief Risk Office

Indemnities for fraud cases are to be approved by either Fraud Risk Manager or Chief Risk Officer, regardless of the amount.

All fraud GL's are to be reconciled each month (current & YTD) and recorded in TriLine monthly with a description of the loss reason/s.

Appendix 1 Examples of common types of fraud and acts of corruption

Cyber Fraud

Advance fee fraud

• Cheating victims out of money by promising them an eventual payoff. The scammer emails his victim with news of some financial windfall, often represented as the wealth of a distant relative or the remnants of some other illicit fortune. All the victim needs to do to claim this wealth is provide some identifying information and pay a few incidental expenses. The lure of easy wealth has found many victims for the perpetrators of these frauds, with some individual marks losing thousands, or even hundreds of thousands of dollars.

Identity Takeover

• The fastest growing type of fraud – where a genuine identity is stolen from an individual and misused for financial gain.

Online Credit Applications

• Fraudulent online credit applications by falsifying information to obtain a favorable outcome.

Social Engineering Fraud

• Techniques such as 'spear phishing', where cybercriminals hook their victims with a malware-infected email that appears to be from a trusted individual or business and then trick them in to making fraudulent payment requests.

Asset misappropriation

Theft of cash

• Stealing from petty cash.

• Taking money from the till.

• Skimming of cash before recording fees and charges collected (understating fees and charges).

• Stealing incoming cash or cheques through an account set up to look like a bona fi de payee.

False payment requests

• Employee or external fraudsters creating false payment instruction with forged signatures and submitting it for processing.

• False email payment request together with hard copy printout with forged approval signature.

• Taking advantage of the lack of time which typically occurs during end of the month processing to get false invoices approved and paid.

Cheque fraud

• Theft of counter cheques.

• Duplicating or counterfeiting of cheques.

• Tampering with cheques (payee/amount).

• Depositing a cheque into a third party account without authority.

• Cheque kiting (a fraud scheme using two deposit accounts to withdraw money illegally from the bank).

Misuse of accounts

• Money transfer fraud (fraudulent transfers into bank accounts).

• Employee account fraud (where an employee is also a customer and the employee makes unauthorised transactions to their own account

• Stealing passwords to payment systems and inputting series of payments to own account.

* Refunding your own (or family, friend, colleagues) fees when they are not entitled to be refunded.

Payroll

• Fictitious (or ghost) employees on the payroll.

• Falsifying work hours to achieve fraudulent overtime payments.

• Abuse of incentive schemes by manipulating sales figures

• Improper changes in salary levels.

• Abuse of holiday leave or time off entitlements.

• Submitting inflated or false expense claims.

• Adding private expenses to legitimate expense claims.

Inventory and fixed assets

• Theft of inventory.

• False write offs and other debits to inventory.

• Theft of fixed assets, including computers and other

IT related assets.

• Theft or abuse of proprietary or confidential information (customer information, intellectual property, business plans, etc).

Procurement

• Altering legitimate purchase orders.

• Forging signatures on payment authorisations.

• Submitting for payment false invoices from fictitious or actual suppliers.

• Intercepting payments to suppliers.

• Sale of critical bid information, contract details or other sensitive information

Fraudulent statements

Loan Applications

- Customers or brokers falsifying information i.e. overstating length of employment, residency, income & assets or understating liabilities and expenses to obtain a favorable outcome.
- Employees falsifying or withholding information on credit applications in order to meet sales targets.

* Employees providing false documents to support their own personal loan application or to support an application for their customer.
* Churning customers loans to boost sales figures with no benefit to the customer.

Financial

- Improper revenue recognition
- Improper classification of revenues.

Misstatement of assets, liabilities and/or expenses

- Fictitious fixed assets.
- Overstating assets acquired through merger and acquisitions.
- Improper capitalisation of expenses as fixed assets (software development, research and development, start up costs, interest costs, advertising costs).
- Manipulation of fixed asset valuations.
- Schemes involving inappropriate depreciation or amortisation.
- Incorrect values attached to goodwill or other intangibles.
- Fictitious investments.
- Improper investment valuation (misclassification of investments, recording unrealised investments, declines in fair market value/overvaluation).
- Accounts receivable schemes (e.g. creating fictitious receivables or artificially inflating the value of receivables).
- Misstatement of prepayments and accruals.
- Understating loans and payables.
- Fraudulent management estimates for provisions, reserves, impairment etc.
- Off balance sheet items.
- Delaying the recording of expenses to the next accounting period.

Other accounting misstatements

- Misrepresentation of suspense accounts for fraudulent activity.
- Improper accounting for mergers, acquisitions, disposals and joint ventures.
- Improper or inadequate disclosures.
- Fictitious general ledger accounts.
- Journal entry fraud (using accounting journal entries to fraudulently adjust financial statements).
- Concealment of losses.

Corruption

Conflicts of interest

Kickbacks

- Kickbacks to employees by a supplier in return for the supplier receiving favourable treatment.
- Kickbacks to senior management in relation to the acquisition of a new business or disposal of part of the business.
- Employee provides pricing discounts to a customer to receive a kickback.
- Preferential treatment of customers in return for a kickback.

Personal interests

- Collusion with brokers, customers and/or suppliers.
- Favouring a broker or supplier in which the employee has a financial interest.
- Employee setting up and using own consultancy for personal gain (conflicts with the company's interests).
- Employee hiring someone close to them over another more qualified applicant.
- Transfer of knowledge to a competitor by an employee who intends to joins the competitor's company.
- Misrepresentation by insiders with regard to a corporate merger, acquisition or investment.
- Insider trading (using business information not released to the public to gain profits from trading on the stock exchange).

Bribery

- Authorising orders to a particular supplier in return for bribes or personal benefits.
- Giving and accepting payments to favour or not favour other commercial transactions or relationships.
- Anti-trust activities such as price fixing or bid rigging.

Non-financial

- Falsified employment credentials e.g. qualifications and references.