



WESTERN AUSTRALIA
POLICE FORCE

**FRAUD AND CORRUPTION
CONTROL PLAN**



2022 - 2025

| Action | Person | Version | Date |
|---------------------------|--|---------|------------|
| Authored | Michaela Miller | 0.1 | 16/07/2021 |
| Reviewed | Audit and Risk Assurance Committee | 0.2 | 27/07/2021 |
| Reviewed | Diane Konstantinou, Legislation and Policy | 0.2 | 25/08/2021 |
| Amended | Michaela Miller | 1.0 | 25/08/2021 |
| Reviewed | <p>Assistant Commissioners:</p> <ul style="list-style-type: none"> Professional Standards • Operations Support • State Crime • State Intelligence & Command • Regional WA • Metropolitan Region • Operation Tide • Professional Development • Strategy and Legal • Specialist & Support Services <p>Directors:</p> <ul style="list-style-type: none"> • Media and Corporate Communications • Governance & Corporate Support • Finance and Business Services • Human Resources • Asset Management <p>Executive Director</p> <p>Chief Information Officer</p> | 1.0 | 30/08/2021 |
| Amended | Michaela Miller | 1.1 | 20/09/2021 |
| Amended (new Standard) | Michaela Miller | 2.0 | 26/11/2021 |
| Reviewed | <p>Assistant Commissioners:</p> <ul style="list-style-type: none"> • Professional Standards • Operations Support • State Crime • State Intelligence & Command • Regional WA • Metropolitan Region • Operation Tide • Professional Development • Strategy and Legal • Specialist & Support Services <p>Directors:</p> <ul style="list-style-type: none"> • Media and Corporate Communications • Governance & Corporate Support • Finance and Business Services • Human Resources • Asset Management <p>Executive Director</p> <p>Chief Information Officer</p> | 2.0 | 20/12/2021 |
| Amended | Michaela Miller | 2.1 | 07/02/2022 |

CONTENTS

| | |
|--|-----------|
| 1. Introduction | 4 |
| 1.1 Purpose | 4 |
| 1.2 Police officers and police staff – one public sector agency | 5 |
| 1.2.1 The Public Sector Commission | 5 |
| 1.2.2 Commissioner’s Instructions | 5 |
| 1.2.3 Public Sector Standards | 5 |
| 2. Definitions | 6 |
| 2.1 Fraud | 6 |
| 2.2 Corruption | 6 |
| 2.3 Technology-enabled fraud | 6 |
| 2.4 Bribery | 6 |
| 2.5 Integrity | 7 |
| 2.6 Unethical Behaviour | 7 |
| 2.7 Misconduct, serious misconduct and police misconduct | 7 |
| 2.7.1 Serious misconduct | 7 |
| 2.7.2 Misconduct | 7 |
| 2.7.3 Police misconduct and reviewable police action | 8 |
| 3. Planning and resourcing | 9 |
| 3.1 Program for fraud control planning and review | 9 |
| 3.2 Roles and accountabilities for fraud and corruption control | 9 |
| 3.2.1 Commissioner of Police | 9 |
| 3.2.2 Corporate Executive | 9 |
| 3.2.3 Senior Managers and Line Managers | 9 |
| 3.2.3.1 Regional and remote District Offices | 10 |
| 3.2.4 Audit and Risk Assurance Committee | 10 |
| 3.2.5 Assistant Commissioner Professional Development | 11 |
| 3.2.6 Public Interest Disclosure officers | 11 |
| 3.2.7 WA Police Force employees | 11 |
| 3.3 Internal audit activity in fraud and corruption control | 11 |
| 3.4 Risk Management Unit | 11 |
| 3.5 External assistance | 12 |
| 4. Fraud and corruption prevention | 13 |
| 4.1 Integrity framework | 13 |
| 4.1.1 Code of Ethics – Public sector requirements | 13 |
| 4.1.2 Code of Ethics – Police Act and Regulations | 13 |
| 4.1.3 One public sector agency – a single Code of Conduct | 13 |
| 4.1.4 Integrity Strategy for WA Public Authorities | 13 |
| 4.1.5 Policies and procedures | 14 |
| 4.1.6 Legislation | 15 |
| 4.2 Integrity in decision making | 15 |
| 4.3 Internal control | 16 |
| 4.3.1 Pressure testing the internal control system | 16 |

| | | |
|-----------|---|-----------|
| 4.4 | Risk assessment | 17 |
| 4.5 | Fraud and corruption risks within law enforcement | 18 |
| 4.6 | Communication, training and awareness | 18 |
| 4.7 | Financial management | 19 |
| 4.8 | Procurement management | 19 |
| 4.9 | Policy development | 19 |
| 4.10 | Information security management | 19 |
| 4.11 | Workforce screening | 19 |
| 4.12 | Record keeping and confidentiality of information | 20 |
| 4.13 | Security clearances | 20 |
| 4.14 | Performance management and role accountability | 20 |
| 4.15 | Performance based targets | 21 |
| 4.16 | Conflict of interest | 21 |
| 4.17 | Secondary employment | 21 |
| 4.18 | Declarable associations | 21 |
| 4.19 | Gifts, benefits and hospitality | 21 |
| 4.20 | Drug and alcohol testing | 21 |
| 4.21 | Integrity testing | 21 |
| 4.22 | Leave and job rotation | 22 |
| 4.23 | Supplier and customer integrity | 22 |
| 5. | Fraud and corruption detection | 23 |
| 5.1 | Fraud and corruption detection program | 23 |
| 5.2 | Audit | 23 |
| 5.2.1 | Internal audit | 23 |
| 5.2.2 | Role of external auditors | 23 |
| 6. | Reporting Mechanisms | 24 |
| 6.1 | Reporting suspected fraud and corruption | 24 |
| 6.1.1 | Employee reporting options (internal) | 24 |
| 6.1.2 | Reporting to WA Police Force (contractors and public) | 24 |
| 6.1.3 | Reporting to oversight and external bodies | 24 |
| 6.2 | Complaint management | 25 |
| 6.3 | Intelligence collection | 25 |
| 6.4 | Whistleblower protection | 25 |
| 6.4.1 | Supported Internal Witness Program | 25 |
| 6.4.2 | Public Interest Disclosure | 25 |

| | |
|--|-----------|
| 7. Responding to fraud and corruption incidents | 26 |
| 7.1 Procedures for the investigation of detected or suspected incidents..... | 26 |
| 7.1.1 Response procedure..... | 26 |
| 7.2 Internal reporting and escalation..... | 26 |
| 7.3 Disciplinary procedures..... | 27 |
| 7.4 Procedural fairness..... | 27 |
| 7.5 Confidentiality..... | 27 |
| 7.6 Proceedings to recover the proceeds of fraud or corruption..... | 27 |
| 7.7 Internal control review following discovery of fraud..... | 27 |
| Authority | 28 |
| Primary Contact:..... | 28 |
| Plan Owner:..... | 28 |
| Appendix 1 - The Fraud Triangle | 28 |
| The Executive Fraud Triangle..... | 29 |
| Appendix 2 - Examples of Fraudulent and Corrupt Conduct | 30 |
| Forms of corruption..... | 30 |
| Appendix 3 - Red Flags of Fraudulent and Corrupt Conduct | 34 |
| Opportunity Red Flags: Employees Against the Company..... | 34 |
| Opportunity Red Flags: Individuals on Behalf of the Company..... | 34 |
| Personal Characteristic Red Flags..... | 35 |
| Situational Pressure Red Flags: Employees Against the Company..... | 35 |
| Situational Pressure Red Flags: Management on Behalf of the Company..... | 35 |

1. INTRODUCTION

The Western Australia Police Force has zero tolerance of fraud, corruption or misconduct, and is committed to the highest standards of transparency, probity and accountability.

This stance aligns with the WA Police Force vision *'to be an exceptional Police Force for our community'* and mission *'to provide trusted and valued policing for Western Australia'*, with all our employees enacting our values of Duty, Teamwork, Integrity and Care.

All employees have a duty to report misconduct and unethical behaviour, and these reports will be investigated and resolved in accordance with WA Police Force policies and procedures, and the *Corruption, Crime and Misconduct Act 2003* (CCM Act). All legal obligations to the principles of procedural fairness¹ will be met.

The WA Police Force is accountable to the Government of Western Australia and upholds the Public Sector Code of Ethics principles² of:

- **Personal Integrity** – we act with care and diligence and make decisions that are honest, fair, impartial, and timely, and consider all relevant information.
- **Relationships with others** – we treat people with respect, courtesy and sensitivity and recognise their interests, rights, safety and welfare.
- **Accountability** – we use the resources of the state in a responsible and accountable manner that ensures the efficient, effective and appropriate use of human, natural, financial and physical resources, property and information.

All employees share in the collective responsibility to assess the risk of fraud and corruption in the activities undertaken in their business area, identify and report suspected fraud or corruption, and behave ethically and promote a culture of integrity in the workplace. Victimisation of individuals who report fraud, corruption or misconduct will not be tolerated by the WA Police Force.

The Western Australia Police Force Fraud and Corruption Control Plan (the Plan) has been developed in accordance with *Australian Standard AS8001-2021 Fraud and Corruption Control*, and applies to all employees, permanent, temporary, contract and casual staff, volunteers and other Government sector employees who are on secondment or assigned to the WA Police Force.

1.1 Purpose

The Plan:

- describes what fraud and corruption is and how it can impact on the functions and service delivery by the WA Police Force
- describes roles and responsibilities of individuals and business areas within the WA Police Force regarding the management of fraud and corruption
- describes the process of reporting fraud and corruption, including escalation paths
- illustrates how the principles in AS 8001:2021 Fraud and Corruption Control translate to action within the WA Police Force
- describes how reports of fraud and corruption are investigated or referred

¹ Procedural fairness (natural justice) Guidelines. Ombudsman Western Australia

² Commissioner's Instruction No. 7: Code of Ethics. Public Sector Commission. Government of Western Australia

1.2 Police officers and police staff – one public sector agency

Within the WA Police Force, personnel are predominantly employed under the following legislative instruments:

- *Police Act 1892* (police officers and auxiliary officers)
- *Public Sector Management Act 1994* (public servants)

Under s4 *Public Sector Management Act 1994* the Commissioner of Police is deemed to be the chief executive officer of the WA Police Force.

Being employed under different Acts, and industrial agreements and awards which may mean different processes, entitlements, rules and regulations can apply to certain circumstances. Managers and supervisors are required to understand these differences.

1.2.1 The Public Sector Commission

The role of the Public Sector Commission (PSC) is described in legislation, including the PSM Act, as strengthening the efficiency, effectiveness and capability of the public sector to meet existing and emerging needs. This also includes maintaining and advocating for public sector professionalism and integrity.

1.2.2 Commissioner's Instructions

The Public Sector Commissioner issues instructions for public sector agencies and employees regarding a broad range of management and administration matters. While mandatory for the majority of public sector departments, Schedule 1 of the PSM Act provides that the WA Police Force is an entity which is not an organisation under the Act. Due to this, some of the Commissioner's Instructions are not mandatory for the WA Police Force as an organisation, while still being applicable to employees under the PSM Act. In the interests of minimising administrative duplication, some Instructions covering police staff are developed as corporate initiatives applicable to all employees, including police officers. Examples of this include, CI No. 7: Code of Ethics and CI No. 8: Codes of conduct and integrity training.

1.2.3 Public Sector Standards

Under s.21 of the PSM Act the Public Sector Commissioner establishes minimum standards of merit, equity and probity that the public sector has to comply with. The standards are principle-based, and collectively referred to the Public Sector Standards in Human Resource Management. The six Standards are:

1. Employment
2. Performance Management
3. Grievance Resolution
4. Redeployment
5. Termination
6. Discipline

In the case of these Standards, the WA Police Force has provided *"Police officers are not covered by the Public Sector Standards in Human Resource Management; however, the general principles contained in the standards will be applied to them"* (HR-18.01 General Principles of Human Resource Management).

2. DEFINITIONS

2.1 Fraud

The WA Police Force has adopted the following definition of fraud, contained in the Australian Standard: Fraud and Corruption Control AS 8001-2021 as:

'dishonest activity causing actual or potential gain or loss to any person or organisation including theft of moneys or other property by persons internal and/or external to the organisation and/or where deception is used at the time, immediately before or immediately following the activity.'

In addition to this definition, the following applies:

- Property in this context also includes intellectual property and other intangibles such as information.
- Fraud 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.
- While conduct must be dishonest for it to meet the definition of “fraud” the conduct need not necessarily represent a breach of the criminal law.
- The concept of fraud within the meaning of AS8001:2021 can involve fraudulent conduct by internal and/or external parties targeting the organisation or fraudulent or corrupt by the organisation itself targeting external parties.

2.2 Corruption

The WA Police Force has adopted the following definition of corruption contained in the Australian Standard: Fraud and Corruption Control AS 8001-2021 as:

'Dishonest activity in which a person associated with an organisation (e.g. director, executive, manager, employee or contractor) acts contrary to the interests of the organisation and abuses their position of trust in order to achieve personal advantage or advantage for another person or organisation. This can also involve corrupt conduct by the organisation, or a person purporting to act on behalf of and in the interests of the organisations, in order to secure some form of improper advantage for the organisation either directly or indirectly.'

For the purposes of the WA Police Force, this means the acts of any member of the Police Force, or any employee or contractor of the WA Police Force.

2.3 Technology-enabled fraud

The WA Police Force has adopted the following definition of technology-enabled fraud contained in the Australian Standard: Fraud and Corruption Control AS 8001-2021 as:

'Fraud against or by an organisation which relies heavily on information technologies and which would not be possible without information technologies.'

The concept of technology-enabled fraud types follows the binary classification of cyber-enabled and cyber-dependent crimes in which the former include frauds made possible through the use of technologies, while the latter are so-called “pure” cybercrimes that require the presence of technologies for their commission – such as access and disruption offences.

2.4 Bribery

The WA Police Force has adopted the following definition of bribery contained in the Australian Standard: Fraud and Corruption Control AS 8001-2021 as:

'Offering, promising, giving, accepting or soliciting of an undue advantage of any value (which could be financial or non-financial), directly or indirectly, and irrespective of location(s), in violation of applicable law, as an inducement or reward for a person acting or refraining from acting in relation to the performance of that person's duties.'

The Australian Standard considers:

- bribery to be a subset of corruption; and
- that all instances of bribery will constitute corruption; but
- that not all instances of corruption will constitute bribery.

2.5 Integrity

Integrity refers to the expected standards of conduct and behaviour of employees which reflect honesty, accountability, transparency, impartiality, and acting with care and diligence.

2.6 Unethical Behaviour

Actions or behaviours that contravene the WA Police Force Code of Conduct, or meet the definitions of misconduct, serious misconduct or reviewable police action, as defined by the CCM Act.

2.7 Misconduct, serious misconduct and police misconduct

The WA Police Force has adopted the definitions of misconduct, serious misconduct and reviewable police action contained within the CCM Act.

2.7.1 Serious misconduct

As defined by the CCM Act serious misconduct means —

- (a) misconduct of a kind described in section 4(a), (b) or (c) by a public officer; or
- (b) police misconduct;

2.7.2 Misconduct

As defined by the s.4 of CCM Act, misconduct occurs if —

- (a) a public officer corruptly acts or corruptly fails to act in the performance of the functions of the public officer's office or employment; or
- (b) a public officer corruptly takes advantage of the public officer's office or employment as a public officer to obtain a benefit for himself or herself or for another person or to cause a detriment to any person; or
- (c) a public officer whilst acting or purporting to act in his or her official capacity, commits an offence punishable by 2 or more years' imprisonment; or
- (d) a public officer engages in conduct that —
 - (i) adversely affects, or could adversely affect, directly or indirectly, the honest or impartial performance of the functions of a public authority or public officer whether or not the public officer was acting in their public officer capacity at the time of engaging in the conduct; or
 - (ii) constitutes or involves the performance of his or her functions in a manner that is not honest or impartial; or
 - (iii) constitutes or involves a breach of the trust placed in the public officer by reason of his or her office or employment as a public officer; or
 - (iv) involves the misuse of information or material that the public officer has acquired in connection with his or her functions as a public officer, whether the misuse is for the benefit of the public officer or the benefit or detriment of another person,

and constitutes or could constitute —

- (v) [deleted]
- (vi) a disciplinary offence providing reasonable grounds for the termination of a person's office or employment as a public service officer under the *Public Sector Management Act 1994* (whether or not the public officer to whom the allegation relates is a public service officer or is a person whose office or employment could be terminated on the grounds of such conduct).

2.7.3 Police misconduct and reviewable police action

Police misconduct means —

- (a) misconduct by —
 - (i) a member of the WA Police Force; or
 - (ii) an employee of the Police Department; or
 - (iii) a person seconded to perform functions and services for, or duties in the service of, the Police Department;

or

- (b) reviewable police action;

Reviewable police action means any action taken by a member of the WA Police Force, an employee of the Police Department or a person seconded to perform functions and services for, or duties in the service of, the Police Department that —

- (a) is contrary to law; or
- (b) is unreasonable, unjust, oppressive or improperly discriminatory; or
- (c) is in accordance with a rule of law, or a provision of an enactment or a practice, that is or may be unreasonable, unjust, oppressive or improperly discriminatory; or
- (d) is taken in the exercise of a power or a discretion, and is so taken for an improper purpose or on irrelevant grounds, or on the taking into account of irrelevant considerations; or
- (e) is a decision that is made in the exercise of a power or a discretion and the reasons for the decision are not, but should be, given.

3. PLANNING AND RESOURCING

3.1 Program for fraud control planning and review

The WA Police Force organisational values and culture, governance and risk management framework and controls, work together to prevent, detect and respond to potential or actual fraudulent or corrupt conduct.

The Plan shall be reviewed at least every two years; however, a review can be triggered at any time by changes in the Australian Standard for Fraud and Corruption Control (updated in June 2021), or any legislative or operational requirement.

All Portfolios and Directorates should apply the appropriate amount of resources to manage their own level of fraud and corruption risk.

3.2 Roles and accountabilities for fraud and corruption control

It is the responsibility of all WA Police Force personnel to act ethically and minimise the possibility of fraud and corruption. This includes managing fraud and corruption related risks relevant to their role, and ensuring the continued operation of controls to prevent fraud and corruption. This responsibility encompasses the immediate reporting of any known or suspected fraudulent or corrupt activity.

3.2.1 Commissioner of Police

The Commissioner of Police has responsibility for the effective and economical use of the agency's resources and for determining appropriate controls in managing fraud and corruption risks in the department.

This responsibility is appropriately delegated to the Executive, senior managers and line managers through the WA Police Force Administrative Delegations Schedule.

Under the CCM Act, the Commissioner of Police is required to notify the Corruption and Crime Commission (CCC) if misconduct, fraud or corruption is suspected.

3.2.2 Corporate Executive

The Corporate Executive comprises of the Commissioner of Police, Deputy Commissioners and the Executive Director. The Corporate Executive will:

- maintain, model and foster the highest standards of ethical behaviour in accordance with the Western Australia Police Force Code of Conduct, applicable Public Sector Standards and Commissioner's Instructions
- demonstrate ethical and accountable decision making
- ensure agreed strategies are implemented at portfolio and directorate level

3.2.3 Senior Managers and Line Managers

Senior managers and line managers are responsible for ensuring the Plan is effectively implemented within their business units. They must:

- provide leadership, guidance and support to employees in preventing fraud and corruption and modelling ethical behaviour
- create and foster a culture that encourages open discussion about fraud and corruption related risks
- set/enforce disciplinary standards
- identify high fraud and corruption risk areas
- identify specific sources of fraud or corruption risk
- participate in fraud and corruption risk assessment reviews
- implement remedial action to address issues identified by the fraud and corruption risk assessment reviews
- assess the cost/benefit of introducing anti-fraud and corruption procedures;

- develop/modify practices to reduce fraud and corruption risk
- monitor the continued operation of controls to prevent fraud and corruption
- receive reports of suspected fraud or corruption from employees and taking appropriate steps to address concerns reported
- report suspected fraud and corruption promptly and maintain confidentiality
- ensure the protection of complainants who report fraudulent or corrupt activities.

3.2.3.1 Regional and remote District Offices

Fraud and corruption events often occur in business operations geographically remote from the organisation's central management. District Superintendents are accountable for fraud and corruption control within the business units under their command.

3.2.4 Audit and Risk Assurance Committee

The objective of the WA Police Force Audit and Risk Assurance Committee (ARAC) is to provide independent advice and assurance on WA Police Force's governance, risk, control and compliance frameworks, internal audit activities and its annual financial reporting responsibilities/obligations.

In regard to fraud and corruption controls, the Committee will:

- Review whether the WA Police Force has in place a current and comprehensive risk management framework, and associated procedures for the effective identification and management of the agency's key financial and operational risks, including fraud
- Review the process for developing and implementing the agency's fraud control arrangements and seek satisfaction that the agency has appropriate processes and systems in place to detect, capture and effectively respond to fraud risks
- Review reports on fraud from management that outline any significant or systemic allegations of fraud, the status of any ongoing investigations and any changes to identified fraud risk in the entity

The Assistant Commissioner Professional Standards is the designated Executive Sponsor for fraud and corruption control. The AC Professional Standards is responsible for the implementation of fraud and corruption prevention strategies and processes for the prevention, detection and investigation of fraud and corruption.

Accountabilities include:

- prevention activities including fraud risk assessments and improvement of controls
- monitoring the reporting, management and investigation of reports of fraud and/or corruption
- initiating investigations with regard to fraud or corruption
- reporting to the ARAC on matters relating to fraud and corruption
- keeping informed of current developments and issues in fraud and corruption control generally and disseminating relevant best-practice information throughout the organisation as appropriate
- sharing knowledge and facilitating the adoption of better practices on fraud and corruption related risk management across the agency
- ongoing review of fraud and corruption control policies, plans and initiatives to enhance fraud and corruption related risk management
- maintaining the following records and statistical data to support reporting purposes, and the evaluation of the effectiveness of fraud and corruption control strategies including:
 - the number of reports and/or allegations of fraud and/or corruption received; and
 - details of how the matters were progressed (review and reform of administrative processes/procedures, disciplinary action or criminal prosecution).

3.2.5 Assistant Commissioner Professional Development

Professional Development is responsible for developing training and training related communication initiatives to support ongoing fraud and corruption related risk awareness, as requested.

3.2.6 Public Interest Disclosure officers

Public Interest Disclosure (PID) officers will investigate information disclosed, or cause that information to be investigated, and take action following the completion of the investigation in accordance with the relevant provisions of the *Public Interest Disclosure Act 2003* (PID Act). The PID Act provides protection for those making such disclosures and those who are the subject of disclosures.

3.2.7 WA Police Force employees

All employees have a responsibility to contribute to preventing fraud and corruption by acting ethically; complying with controls, policies and procedures, and reporting suspected incidences of misconduct, and fraudulent or corrupt behaviour through reporting mechanisms. The agency will provide support and protection to any employee who reports incidences of fraud and corruption.

All employees should:

- embrace and foster an ethical work-place culture
- recognise the value and importance of personally contributing to fraud and corruption prevention
- develop an understanding of good work practices, systems and controls
- keep abreast of best practices for preventing fraud and corruption, specific to their roles
- become aware of the different types of fraud and corruption that can occur in the workplace and how to detect them
- report suspected incidences of fraudulent or corrupt conduct in accordance with policies and procedures.

3.3 Internal audit activity in fraud and corruption control

The WA Police Force Management Audit Unit (MAU) plays an important role in identifying weaknesses in the fraud and corruption control environment.

Internal Audit operates under the *International Professional Practices Framework* (IPPF) issued by the Institute of Internal Auditors in Australia. The International Standards Practice of Internal Auditing (Standards) provides the key operating element of the IPPF.

Internal auditors must exercise professional care (Standard 1220.A1) to consider potential fraud risk and have sufficient knowledge to evaluate the risk of fraud and the manner in which this is managed by the organisation (Standard 1210.A2). They are obligated to look out for or consider potential fraud risks to the organisation. To achieve this, internal auditors must consider the probability of fraud when developing the engagement objectives (Standard 22.10.A2). If an internal auditor locates a fraud or identifies a potential fraud risk or exposure, they must then report this to senior management and the ARAC (Standard 2060).

3.4 Risk Management Unit

The Risk Management Unit delivers the Enterprise Risk Management Framework to guide the identification, management and reporting of operational, corporate and strategic risks. The Unit is also responsible for the development and cyclic review of agency business continuity plans under the Business Continuity framework. The:

- Organisational Risk Management Program that relates to the identification, assessment, treatment, monitoring and reporting of risks to support the achievement of the agency's strategic directions, frontline policing and local planning priorities
- Organisational Business Continuity Program that relates to the identification of the agency's critical functions and associated key business activities, and the development/rehearsal of specific plans to respond effectively to unwanted disruptions to those functions and activities.

3.5 External assistance

The CCC works in collaboration with government agencies to educate, prevent, assess and investigate fraud and corruption in the public sector.

Where a resource need cannot be satisfied internally, due to factors such as limited capability, conflict of interest or operational requirements, the Assistant Commissioner of Professional Standards, may source the following services externally:

- forensic accounting
- computer forensic analysis
- data analytics
- fraud risk assessments
- preliminary investigation interviews
- Support to complete investigations.

Cost associated with engaging external service providers is borne by the Portfolio or Directorate where the work is necessary to be undertaken. Consultation with the relevant Assistant Commissioner or Director is required.

4. FRAUD AND CORRUPTION PREVENTION

4.1 Integrity framework

The Plan is part of the WA Police Force's commitment to maintaining a fraud and corruption integrity framework. The approach outlined in this document forms an integral part of the agency's corporate, strategic and operational planning processes and objectives.

4.1.1 Code of Ethics – Public sector requirements

Section 9 of the PSM Act requires all public sector bodies and employees to comply with the provisions of public sector standards and Code of Ethics. The Act also requires public sector bodies and employees to act with integrity when performing official duties and to exercise courtesy, consideration and sensitivity in dealings with employees and members of the public.

4.1.2 Code of Ethics – Police Act and Regulations

The expectations of ethical behaviour, duties and discipline for police officers and auxiliary officers are provided in the *Police Act 1892* and the Police Force Regulations 1979.

4.1.3 One public sector agency – a single Code of Conduct

Irrespective of employment status and the underpinning legislative and regulatory instruments, all employees are subject to the Western Australia Police Force Code of Conduct (2020).

The Code of Conduct applies to all employees, regardless of rank or position, including employees who are permanent, consultants, volunteers, casual, contractors or any other group or individual who is engaged with the WA Police Force.

The WA Police Force Integrity Framework is a manual for WA Police Force managers, supervisors, subject officers, witnesses and external stakeholders describing the procedures adopted by the WA Police Force when investigating Police Misconduct and Police Staff Breaches of Discipline.

4.1.4 Integrity Strategy for WA Public Authorities

The WA Police Force aligns to the Public Sector Commission's *Integrity Strategy for WA Public Authorities 2020-2023*, to ensure:

- Effective governance systems and frameworks are established
- A culture of integrity exists, and is reinforced and communicated by leaders
- Individual and authority integrity knowledge, skills and competence are grown
- Prevention, detection and response to integrity matters are everyone's personal and professional responsibilities.

4.1.5 Policies and procedures

The following plans, policies and documents regulate appropriate practices and behaviours, and should be read in conjunction with this document:

- AA-01.00 Code of Conduct
- AD-06.13 Contracts - Procurement of Goods and Services
- AD-16.06 Duties and Responsibilities of Members (Generally)
- AD-16.13 Blueline
- AD-16.15 Professional Standards Information Management System
- AD-54.00 Sponsorships and Donations
- AD-63.00 Discounted Goods and Services Offered to Police Officers
- AD-68 Stand Down and Suspension of Members
- AD-71.00 Information Security Policy
- AD-71.02 Computer and Internet Access
- AD-85.00 Information Release and Sharing
- AD-84.04 Gifts, Benefits and Hospitality
- AD-84.10 Conflicts of Interest
- AD-96.01 Declarable Association Register
- AD-52.01 Records Management Policy
- AD-66.00 Financial Management Manual
- AD-74.00 Supported Internal Witness
- AD-91.00 Personnel Security Vetting
- AD-95.00 Risk Management
- FC-01.00 Formation of Contracts
- HR-01.01 Employee Employment Records
- HR-07 Leave
- HR-09 Flexible Work Practices
- HR-12.00 Secondary Employment
- HR-14 Vacancies, Transfers, Reliefs and Promotions
- HR-15 Police Recruiting
- HR-20.01 Hours of Duty
- HR-23.01 Recruitment and Selection for Police Staff Positions
- HR-24.01 Discipline of Police Staff
- HR-27.00 Performance Management
- LO-01.06 Restricted Access to Information on Police Computer Systems
- SI-01.01 Protection of Authorised Covert Business Requirements and Activities
- EX-11.00 Human Source Management
- Western Australia Police Force Integrity Framework (Ethical Standards Division)
- Risk Management Framework
- Financial and Asset Management Manual

- Good Governance Practice Guide (Management Audit Unit)
- Information Security Standards and Guidelines (Security and Risk Unit)
- ADS-1 Human Resource Management and Administration Delegation Schedule (Human Resources Directorate)
- Public interest disclosure procedures and guidelines for the Western Australia Police Force (Internal Affairs Unit)
- Protective Security Policy Framework (Commonwealth Government)

4.1.6 Legislation

Relevant legislation includes (but not limited to):

- *Public Sector Management Act 1994*
- *Police Act 1892*
- Police Force Regulations 1979
- *Corruption, Crime and Misconduct Act 2003*
- *Criminal Code Act Compilation Act 1913*
- *Financial Management Act 2006*
- Financial Management Regulations 2007
- *Industrial Relations Act 1979*
- *Procurement Act 2020*
- *Public Interest Disclosure Act 2003*
- *State Records Act 2000*

4.2 Integrity in decision making

The community of Western Australia expects all public officers to act with integrity when making decisions, including:

- policy decisions
- regulation, enforcement and compliance decisions
- decisions about services and product delivery to the community
- internal governance and management decisions including human resource, financial and procurement decisions
- decisions about the security and appropriate release of information and records.

The Integrity in Decision Making Framework for WA public bodies³ provides key questions in the following areas:

- **Power:** use power responsibly and for its intended purpose
- **Principles:** apply ethical, accountability and proportionality principles
- **Proper process:** follow a proper and appropriate process
- **Proportionate outcomes:** achieve evidence-based outcomes

Decisions will be documented and bear external scrutiny.

Delegated authority relates to the delegation of executive power to carry out administrative actions within an organisation from an executive officer to a nominated officer, therefore transferring responsibility. The authorised, or responsible, officer is ultimately accountable for the decision.

³ Integrity in Decision Making. The Integrity Coordinating Group. June 2011. The ICG comprises of the Public Sector Commission, Corruption and Crime Commission, Ombudsman Western Australia and the Office of the Information Commissioner

4.3 Internal control

The Commissioner and Corporate Executive of the WA Police Force are committed to ensuring an ethical and high-integrity workplace. Any level of fraud or corruption will not be tolerated, and senior management are responsible for conveying and promoting this message to personnel.

All business processes, especially those identified as having higher risk of fraud and corruption, are subject to a rigorous system of internal controls that are documented, reviewed and updated regularly, and understood by relevant employees. Controls cover existing processes, policies, devices, practices or other actions that act to minimise negative risks or enhance positive opportunities

Strong internal controls are important in protecting against fraud and corruption. In many cases where fraud and corruption are detected, it is possible to identify a fundamental control weakness or failure that either allowed the incident to occur or failed to detect it quickly after it occurred.

Line managers are responsible for ensuring appropriate work systems, including internal controls, are established and maintained.

In addition to the WA Police Force Good Governance Practice program, line managers are encouraged to self-audit and test compliance, or consult with Management Audit Unit for advice.

4.3.1 Pressure testing the internal control system

Pressure testing involves an internal or external individual or team initiating a series of test transactions to assess the operational effectiveness of internal controls. This involves the introduction of documents, data or other action consistent with an actual fraud or corruption event, to determine if existing internal controls are operating as intended and are effective in preventing fraud or corruption of the type contemplated, and then observing how existing internal controls respond to such a test transaction. Common vulnerabilities uncovered through pressure testing include:

- Lack of fraud awareness
- Inadequate quality assurance
- Not verifying information or evidence
- A lack of effective oversight
- Weak technology controls
- Inadequate detection controls
- Lack of reporting or reconciliation

The MAU or the Governance and Organisational Risk Management Unit may perform pressure testing activities over internal controls deemed high risk to identify vulnerabilities and provide assurance to the ARAC and Corporate Board, as required.

4.4 Risk assessment

Each business area must systematically identify, assess and review fraud and corruption risks in line with the WA Police Force Risk Management Framework.

The most important outcome of the fraud and corruption risk assessment process is the development of a treatment plan that specifically addresses the risks identified. These measures should be monitored for effectiveness over time.

A risk assessment that addresses fraud and corruption related risk will establish the level, nature, form and likelihood of fraud and corruption related risk exposures. Like any risk assessment process, assessments of fraud and corruption related risk must be conducted as an ongoing, iterative process. This will maximise the opportunity to identify and treat all fraud and corruption related risks. Consideration of risk factors should include both internal and external environments, and should address all business processes.

All business areas are required to identify risks, including fraud and corruption related risks, at least annually under the Good Governance Practice Guide. Areas with high levels of risk must undertake more frequent reviews.

Risk assessment is a process of continuous improvement. When the risk assessment process begins, business areas must attempt to gain an understanding of the various fraud and corruption scenarios that may occur.

Core areas where fraud and corruption related risk must be considered include:

- information technology and information security
- electronic commerce, electronic service delivery and the internet
- outsourced functions and funded service delivery programs
- grants, funding agreements, and other payments or benefits programs
- tendering processes, purchasing and contract management
- procurement, payment of accounts and invoicing
- services provided to the community
- revenue collection
- use of government purchasing cards
- travel allowance and other common allowances
- salaries, leave, attendance, and timekeeping
- property (including intellectual property) and other physical assets including physical security

The outcome of the risk assessment process will be the development of action items designed to mitigate and manage identified fraud and corruption related risks.

Advice and assistance should be sought from the Risk Management Unit, Governance and Corporate Support.

4.5 Fraud and corruption risks within law enforcement

Previous Royal Commissions⁴ and inquiries⁵ into police corruption and misconduct have identified unique cultural and operational opportunities for serious misconduct, fraud and corruption. Risk areas include:

- Workplace culture
- Covert policing
- Human source management
- Liquor and hospitality industry
- Security industry
- Prostitution
- Racing and gaming industries
- Illicit drug supply and use
- Organised crime
- Outlaw Motorcycle Gangs

Management of high fraud and corruption risk areas are responsible for ensuring assessment, action, monitoring and reporting.

External environmental scanning is an important element in identifying risk areas to law enforcement. Environmental scanning should be undertaken systematically, and included identifying and analysing relevant events, trends and drivers. Australian Standard 8001:2021 prefers the PESTLE model for external scanning:

- **P**olitical environment
- **E**conomic environment
- **S**ocial environment
- **T**echnological environment
- **L**egal environment
- **E**nvironmental factors

4.6 Communication, training and awareness

The primary purpose of education and training in the area of fraud and corruption is to raise the general awareness amongst staff about what fraudulent practices are, identify potential fraud, how to report these practices and to make it very clear that fraudulent practices within the department will not be tolerated.

An awareness and training framework for managers and staff will:

- create and maintain awareness of fraud and corruption related risks
- enable staff to identify fraud risks or red flags pertaining to fraudulent activity
- educate staff as to how to report fraud and corruption
- provide periodic reinforcement of fraud control principles.

It is the responsibility of those in positions of leadership or management to promote an ethical culture, and encourage staff to speak out against fraudulent acts, whether committed by staff or others.

⁴ New South Wales Wood Royal Commission - existence and extent of corruption within the New South Wales Police (1995)

Western Australian Kennedy Royal Commission - into whether there has been corrupt or criminal conduct by any Western Australian Police Officer (2002)

Victoria Lawyer X Royal Commission - into the Management of Police Informants (2018)

⁵ Queensland Fitzgerald Inquiry - Commission of Inquiry into Possible Illegal Activities and Associated Police Misconduct (1987)

The Assistant Commissioners of both Professional Standards and Professional Development share a joint responsibility for promoting fraud and corruption awareness throughout the agency.

The Assistant Commissioner Professional Development is responsible for the development and delivery of the Accountable and Ethical Decision Making (AEDM) program, which provides every employee with a general awareness of fraud and corruption and how to respond if this type of activity is detected or suspected.

4.7 Financial management

All employees must comply with the WA Police Force Financial and Asset Management Manual. The policy framework ensures (but is not limited to):

- effective and efficient control over, and use of, financial resources
- effective management of financial risks
- accountability and transparency in financial management

4.8 Procurement management

All employees must comply with the WA Police Force Procurement Policies and Procedures which specify the governance and process requirements to ensure effective and consistent procurement activity within the agency.

4.9 Policy development

The Legislation and Policy Unit is responsible for ensuring the creation and maintenance of legislative environments in which employees can effectively carry out their functions. This includes the development and preparation of legislative solutions and their progression through Departmental, Ministerial and Parliamentary processes.

The Unit also administers the Corporate Knowledge Base for access by all WA Police Force employees and facilitates the development and implementation of corporate policies and Police Manual content that align with the legislative environment and overarching strategic frameworks.

Legislation and Policy also work with internal and external agencies to facilitate the creation, amendment and transfer of Memorandum of Understandings by providing advice and direction to WA Police Force business areas on how to develop and implement these documents.

Policies are an important control in relation to Fraud and Corruption control, and should contain formalised intentions and directions of the WA Police Force, whereby unethical conduct, fraud and corruption is not tolerated.

4.10 Information security management

The WA Police Force continues to assess exposure to technology-enabled fraud.

All employees must comply with the Information Security Standards and Guidelines, which provides the minimum standards in relation to information security, information assets and system access permissions.

4.11 Workforce screening

Pre-employment screening applies to all prospective police officers (recruits) and public sector staff. Recruitment processes require National Police Clearances, citizenship or residency requirements.

Integrity checks include social networking accounts, charges and convictions, family domestic violence history, declarable associations and conflicts of interest.

Some identified positions also require evidence of qualifications, medical clearance, psychological testing, and/or the requirement to obtain and maintain a Security Clearance.

Pre-commencement screening is required for non-employees such as those contracted to fulfil a service or out-sourced function, for example, consultants, project managers, auditors etc.

4.12 Record keeping and confidentiality of information

A function of the Commissioner of Police is to ensure the WA Police Force keeps proper records, subject to the *State Records Act 2000*. The WA Police Force has an obligation to develop a Records Keeping Plan and a Retention and Disposal Schedule, endorsed by the State Records Office.

Documents include any piece of written, printed, or electronic matter that provides information or evidence or that serves as an official record; including a tape, disc or other device or medium on which information is recorded or stored electronically, mechanically, photographically or otherwise.

Records are to be kept for the following:

- Business Process - all the functions, activities and transactions of a business unit and its employees. Includes public administration as well as policing business
- Corporate Record – including, but not limited to, policies, actions, decisions or business transactions

Western Australia Police Force employees must not:

- Access any information in the Western Australian Police Force Computer System for personal reasons
- Disclose any information contained within the Western Australia Police Computer System to any unauthorised person
- Give to any person any information, that has been furnished to them, or obtained in the course of their official duties; or
- Disclose to any other person the contents of any personal files, advertised vacancy files, computer data etc, unless in the course of their official duties; or
- Publicly comment, either verbally or in writing, on any matter; or
- Use for any purpose, other than for the purpose of their official duty, information gained by or conveyed to them through their employment in the Public Service.

To do so is a breach of discipline under both the Police Force Regulations 1979 and the *Public Sector Management Act 1994*.

4.13 Security clearances

Positions deemed high risk or requiring integrity assurance require a Negative Vetting (NV) security clearance. The WA Police Force is an authorised vetting agency and complies with the Commonwealth Protective Security Policy Framework (Personnel Security) requirements. This function is managed by the Personnel Security Vetting Unit, Professionals Standards.

4.14 Performance management and role accountability

The WA Police Force will move toward incorporating fraud and corruption control into the performance management system.

In addition, position description forms for line managers will be contemporised to include specifying the prevention and detection of fraud and corruption as a part of their role.

All position description forms within the agency should include the employee's duty to comply with the WA Police Force Code of Conduct and duty to report wrongdoing.

To confirm understanding of, and compliance with, the Code of Conduct and fraud and corruption control policies, employees should be required to confirm in writing that they have complied with these documents and undertake to comply over the ensuing 12 months.

4.15 Performance based targets

Any performance based targets shall be assessed to minimise risk of unintended consequences of incentivising fraud and/or corruption.

4.16 Conflict of interest

A conflict of interest is a situation arising from conflict between the performance of public duty and private or personal interests⁶. All employees are required to declare conflicts of interest, whether they be actual, perceived or potential. The Internal Affairs Unit holds a register of conflicts of interest on their 'Internal Affairs Professional' case management system (known as IAPro).

4.17 Secondary employment

Approval to participate in secondary employment is mandatory for police officers (r.621 Police Force Regulations 1979) and public sector staff (s.102 *Public Sector Management Act 1994*). High risk applications are escalated to the Assistant Commissioner Professional Standards. Approval expires on transfer, promotion or change to secondary employment. The Internal Affairs Unit holds a register of secondary employment on IAPro.

4.18 Declarable associations

All employees are required to declare certain associations. This includes any individual, group, or entity which is alleged, known or reputed to be engaging in (or has previously engaged in, or to have expressed an intent to become engaged in) criminal or illegal activities, or activities that are otherwise incompatible or inconsistent with the values and principles of the WA Police Force.

Should the association become publicly known, it may:

- cast doubt on the employee's judgement, loyalty, decision-making and/or ability to resolve integrity issues in favour of their public duty
- create a perception in the mind of a reasonable person that the association is inappropriate and/or the individual has used, may misuse, or may be approached or encouraged to misuse their position within the WA Police Force
- undermine community confidence in the WA Police's ability to maintain integrity and fulfil its mission to provide trusted and valued policing for Western Australia
- otherwise adversely impact on the good standing and reputation of the individual and/or the agency

4.19 Gifts, benefits and hospitality

All employees are to record gifts, benefits and hospitality. Amounts under \$100 are registered within the business area. Amounts exceeding \$100 are reportable to the Ethical Standards Division and are recorded on a central register (IAPRo).

Employees are prohibited from soliciting gifts, benefits and hospitality by using their employment with the WA Police Force.

4.20 Drug and alcohol testing

Police officers have been subject to random drug and alcohol testing since 2011 under Police Force (Member Testing) Regulations 2011. The WA Police Force is currently progressing a policy for all employees under the *Public Sector Management Act 1994* to be subject to random testing.

4.21 Integrity testing

The ability to conduct integrity testing in relation to WA Police Force employees is regulated by the *Criminal Investigation (Covert Powers) Act 2012*.

⁶ Conflicts of Interests: Guidelines for the Western Australia Public Sector. The Integrity Coordinating Group

4.22 Leave and job rotation

Unwillingness to share duties and reluctance to take leave is a fraud and corruption risk 'red flag'⁷.

The WA Police Force has a leave management policy regarding excess leave entitlements. Leave liability reports are provided to business areas monthly for monitoring and action where required.

Job rotation for police officers is managed through the WA Police Force Tenure policy. While public sector staff are permanently appointed to their positions, the agency encourages acting (higher duties) and secondment opportunities (internal and external) to facilitate movement and development of staff.

4.23 Supplier and customer integrity

While fraud and corruption is often instigated by persons internal to an organisation, it is important to consider that the department may be susceptible to externally instigated fraud or corruption. The risk of fraud and corruption is reduced when the department knows who it is dealing with in all significant commercial transactions so the credentials, financial health and integrity of new suppliers or customers is investigated as far as practical, including any conflicts of interest.

When procuring goods and/or services, employees are required to seek competitive quotes from potential suppliers. In addition to ensuring that the submitted offers meet the required specifications and represent value for money, the evaluation process is to include an assessment of the supplier and their disclosure requirements. This includes the identity of the supplier and verification of the company's ABN or ACN.

The rigour of these checks and assessments are to be commensurate with the value and/or risk presented by the procurement. When ordering from a Common Use Arrangement (CUA), suppliers on the panel have already completed a stringent assessment process undertaken by the Department of Finance.

Concerns regarding a supplier's identity or its representation are to be raised with Strategic Procurement and Contracts.

Simple bona fides checks of a supplier should include the following:

- searching open source locations such as the Internet for any adverse news on the supplier and the supplier's key controllers such as the company's owner/s, the Chief Executive Officer and/or its senior manager/s
- consulting with other public departments or private companies who use the supplier to identify any concerns
- evaluating any suspicious activity observed by the department during the life of the relationship, such as presentation of incomplete, incorrect or inflated invoices
- The agency should consider its ongoing commercial relationship with the other party if an inquiry finds a heightened risk of fraud or corruption in continuing to deal with that party. Consideration should also be given to whether new suppliers may have a conflict of interest in their engagement with the department.

⁷ Report 14 Joint Standing Committee on the Corruption and Crime Commission. Red flags...red faces: Corruption risk in public procurement in Western Australia. May 2020

5. FRAUD AND CORRUPTION DETECTION

5.1 Fraud and corruption detection program

The department is committed to identifying, investigating and deterring fraud and corruption in the workplace, and runs a multi-faceted detection program.

The WA Police Force relies on a variety of strategies to minimise the opportunity for fraud and corruption to be committed or to go undetected, including (but not limited to):

- vigilance and awareness of all employees
- internal control systems
- operational risk management processes
- procedures for reporting fraud and corruption
- internal and external audit activities

The WA Police Force is committed to developing maturity in the following fraud and corruption detection actions:

- Post-transactional review
- Analysis of management accounting reports
- Identification of early warning signs
- Data analytics
- Fraud and corruption reporting channels (see Section 6 Reporting Mechanisms)
- Whistleblower protection (see Section 6 – Reporting Mechanisms)
- Leveraging relationships with external parties
- Complaint management
- Exit interviews

5.2 Audit

5.2.1 Internal audit

The WA Police Force Management Audit Unit activities play an important role in identifying weaknesses in the fraud and corruption control environment.

Where it applies to fraud and corruption control, the Professional Practices Framework of the Institute of Internal Auditors is also taken into consideration for individual audit engagements.

5.2.2 Role of external auditors

Australian auditing standards provide for auditing procedures so that the audit will be more likely to detect a material misstatement in financial statements due to fraud or corruption (or error).

The Western Australian Office of the Auditor General's Forensic Audit team conducts joint audits with their performance, financial and information system audit teams. The Office of the Auditor General also conducts targeted audits of public sector entity accounts and matters related to public money, public property and approvals. The Forensic Audit team may also utilise data matching with information received from certain entities, including data that is publicly available. The data matching analysis is only done for audit purposes as mandated by the *Auditor General Act 2006*.

6. REPORTING MECHANISMS

6.1 Reporting suspected fraud and corruption

6.1.1 Employee reporting options (internal)

All WA Police Force employees are required to report suspected fraud and corruption, including possible breaches or suspected breaches of the Code of Conduct, Public Sector Code of Ethics and/or Police Force Regulations 1979 and *Public Sector Management Act 1994*.

Employees may report any suspected fraud and corruption internally via:

- A line manager or supervisor
- District / Divisional Officers (or equivalent)
- Any Assistant Commissioner or Director
- Internal Affairs Unit / Professional Standards Portfolio
- The Blueline (anonymous telephone or email reporting)
- Human Resources
- PID Officers (designated personnel within the WA Police Force)
- Members of the Corporate Executive, including the Commissioner of Police

Irrespective of who the initial report is made to, the Assistant Commissioner of Professional Standards will receive notification.

If the matter is serious and depending on the nature of the suspected fraud or corruption, the agency is required to report to the CCC. Reporting is generally done through Professional Standards, on behalf of the Commissioner of Police.

6.1.2 Reporting to WA Police Force (contractors and public)

The WA Police Force provides an Online Service portal (Police Direct) for any member of the public to report suspected fraud, corruption, misconduct and/or unethical behaviour in relation to WA Police Force employees. Those external to the agency can make a report by any of the following means:

- online complaints form
- by telephone or in person to any police station or district office
- by calling the Police Conduct Investigation Unit
- in writing (email or letter)

Current telephone and address details can be obtained from the Police Direct webpage: www.police.wa.gov.au/Police-Direct - Commendations and Complaints.

If a member of the public is dissatisfied with the management of their report/disclosure, they may report the matter to an external oversight body.

6.1.3 Reporting to oversight and external bodies

There may be reasons an employee, member of the public or any reporter, may be reluctant to report suspected fraud, corruption and/or unethical behaviour directly to the WA Police Force. As there is a duty to report for employees, a number of external reporting options are available, including:

- The Corruption and Crime Commission (option of anonymity)
- A Public Interest Disclosure Officer in an appropriate proper authority:
 - Corruption and Crime Commission (offences under state law)

- Auditor General (substantial unauthorised or irregular use of, or substantial mismanagement of, public resources)
- Ombudsman Western Australia (matters of administration affecting someone in their personal capacity falling within the jurisdiction of the Ombudsman Western Australia)

6.2 Complaint management

The WA Police Force will implement a complaint management system in line with AS/NZS 10002:2014 Guidelines for complaint management in organisations.

All complaints (internal and external) provide valuable intelligence and should be analysed to identify trends and issues.

6.3 Intelligence collection

Reporting employees are not required to evaluate the worth or value of their disclosure. As long as an employee has a reasonable belief that misconduct, fraud and/or corruption may be occurring, a report should be made with as much detail as possible.

Reports that may not have enough detail or information to progress to an investigation still have value in building an intelligence picture. All reports are recorded on IAPro and can be assessed and analysed with other collections.

6.4 Whistleblower protection

6.4.1 Supported Internal Witness Program

The Supported Internal Witness Program (SIWP) is coordinated within the Internal Affairs Unit, Professional Standards. The purpose of the SIWP is to:

- Recognise and support the courageous and ethical stand employees have taken, by voluntarily reporting inappropriate conduct and supporting subsequent investigations
- Develop a professional organisational culture where all employees feel confident to report suspected corruption, unethical conduct, or other 'at risk' behaviours
- Provide practical encouragement and support to the person making the disclosure
- Ensure that appropriate action is taken in relation to the information provided and (in consultation with the investigating officers), provide appropriate feedback to the supported witness, keeping them informed of the status
- Encourage all employees to take responsibility in establishing and maintaining the highest possible standard of ethical behaviour

Support measures offered through the SIWP include:

- Regular contact and support by the SIWP Coordinator or designated SIWP Case Officer
- Working with an identified and suitable local Support Officer, to monitor the workplace for victimisation, harassment or other detriment, threatened or endured
- Referral to Health, Welfare and Safety Division, Peer Support Officers, or the Employee Assistance Program as applicable
- In extreme cases, relocation, or implementation of other protective measures

6.4.2 Public Interest Disclosure

The PID Act encourages people to come forward with information about wrongdoing without fear of reprisal. The PID Act enables people to make disclosures about wrongdoing in the State public sector, local government and public universities without fear of reprisal. It aims to ensure openness and accountability in government by encouraging people to make disclosures and protecting them when they do.

The Public Sector Commission maintains an online directory of PID Officers.

7. RESPONDING TO FRAUD AND CORRUPTION INCIDENTS

7.1 Procedures for the investigation of detected or suspected incidents

The WA Police Force will investigate instances of suspected fraud or corruption, and will assess each matter on its own merits in order to determine next steps. The management of reports is dealt with in WA Police Force Integrity Framework Manual.

All investigations will be conducted in a manner that affords all parties their basic human rights, natural justice and to not circumvent or compromise the established misconduct, disciplinary, managerial or criminal processes. Processes and procedures may vary depending on whether the investigation relates to a police officer or a public servant due to legislative and/or industrial differences in relation to breaches of discipline.

Professional Standards, via the Internal Affairs Unit and the Ethical Standards Division, may conduct, outsource or oversight investigations dependent on the circumstances.

Investigation of unethical conduct, fraud and/or corruption may involve the following core activities:

- interviewing relevant witnesses including obtaining statements where appropriate from witnesses internal and external to the agency
- reviewing and collating documentary evidence
- forensic examination of computer systems
- forensic accounting
- examination of private telephone records (subject to legislation) and agency issued mobile telephones
- enquiries with banks and other financial institutions (subject to legislative requirements)
- enquiries with other third parties
- data search and seizure
- data analytics
- expert witness and specialist testimony
- tracing funds/assets/goods
- preparing briefs of evidence
- liaison with other law enforcement or regulatory agencies
- report preparation

7.1.1 Response procedure

The WA Police Force will develop a procedure for immediate action in response to a fraud and corruption control event.

7.2 Internal reporting and escalation

It is the responsibility of the Assistant Commissioner Professional Standards to report on all fraud and corruption matters within the agency to the Corporate Executive.

Any report of fraud or corruption received by any agency staff member must be relayed to the Professional Standards Portfolio (Ethical Standards Division or the Internal Affairs Unit).

If the matter is urgent and occurs after hours, the Internal Affairs Unit on-call officer can be contacted via the State Operations Command Centre.

Matters involving material loss, media attention, potential political notice, or potential for criminal charges against a staff member should immediately be reported to the Assistant Commissioner Professional Standards during business hours, or the IAU on-call officer after hours.

7.3 Disciplinary procedures

All discipline or misconduct investigations relating to a WA Police Force employee will be conducted in accordance with the *Police Act 1892* and Police Force Regulations 1979 for police officers and the *Public Sector Management Act 1994* for public sector staff. These legislative instruments are operationalised through the WA Police Force Integrity Framework Manual, and for public sector staff, the relevant Public Sector Commission Standards and Instructions.

If during the course of a disciplinary investigation it is determined that criminal offences may have been committed, Professional Standards is to be contacted in the first instance. Criminal investigations have precedence over managerial or disciplinary investigations.

7.4 Procedural fairness

Procedural fairness requires a fair and proper procedure when making a decision, and must be applied in any decision that may negatively affect an existing interest of a person or entity⁸. The rules of procedural fairness require:

- A hearing appropriate to the circumstances
- Lack of bias
- Evidence to support a decision
- Inquiry into matters in dispute

In relation to investigations (7.1) and disciplinary procedures (7.3), the rules of procedural fairness must be adhered to. Procedural fairness also underpins the Public Sector Standards.

7.5 Confidentiality

Confidentiality will be maintained throughout any investigative process.

7.6 Proceedings to recover the proceeds of fraud or corruption

In certain circumstances, legal proceedings may be considered to recover funds or value of assets lost due to fraud, corruption or misappropriation. The Assistant Commissioner Professional Standards will liaise with internal counsel and/or the Director of Public Prosecutions dependent on the circumstances.

Avenues may exist for the agency to undertake civil recovery procedures, or through the criminal court system by way of an application for restitution.

Where there is clear evidence of fraud or corruption, and where the likely benefits of such recovery will exceed the funds and resources invested in the recovery action, then recovery action should be undertaken.

7.7 Internal control review following discovery of fraud

To ensure that any control weaknesses are rectified, a review of the internal control environment should be performed by operational management after an incident of fraud has occurred.

In cases of material fraud, the Management Audit Unit may conduct an internal control review to evaluate the effectiveness of the internal controls in preventing further such incidences. Review outcomes may include the need for:

- new or strengthened controls
- revised policy or procedure
- additional staff training
- increased frequency of internal audit review

Where remediation or enhancements are required, these shall be implemented as soon as practicable.

⁸ Ombudsman Western Australia: Good decision making and practices – Procedural fairness

AUTHORITY

Primary Contact:

Superintendent, Ethical Standards Division, Professional Standards

Plan Owner:

Assistant Commissioner Professional Standards

APPENDIX 1 - THE FRAUD TRIANGLE

Criminologist Donald Cressey is credited with developing the Fraud Triangle (Figure 1), a model explaining the factors that cause someone to commit fraud. It consists of three components which normally must all be present for fraudulent behaviour to occur:

Opportunity

The circumstances that permit someone to commit a fraud, is generally provided through weaknesses in internal control systems such as inadequate or lack of:

- supervision and review
- separation of duties
- management approvals
- system controls

Pressure

The pressure placed on or incentive provided to a person to commit fraud, can be imposed due to:

- personal financial problems
- personal vices such as gambling, drugs, extensive debt, etc
- unrealistic deadlines and performance goals

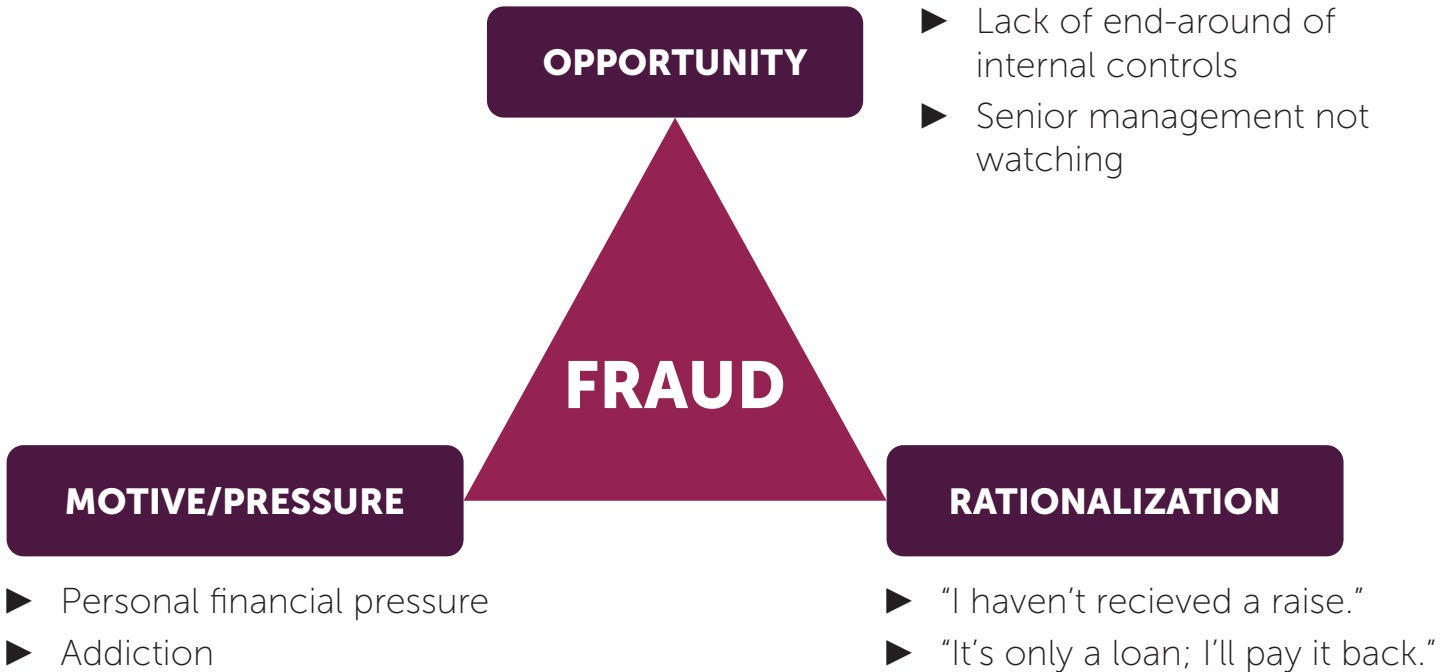
Rationalisation

This occurs when the individual develops a justification for their fraudulent activities where they have a frame of mind or character that allows them to commit a fraud. The rationalisation varies by case and individual. Some examples include:

- “I really need this money and I’ll put it back when I get paid”
- “I’d rather have the organisation on my back than the tax office or creditors”
- “I just can’t afford to lose everything – my home, car, everything”
- “The organisation deserves this for treating me badly”
- “I am entitled to the money”
- “I am underpaid”, or “my employer cheats me”
- “My employer is dishonest to others and deserves to be fleeced”.

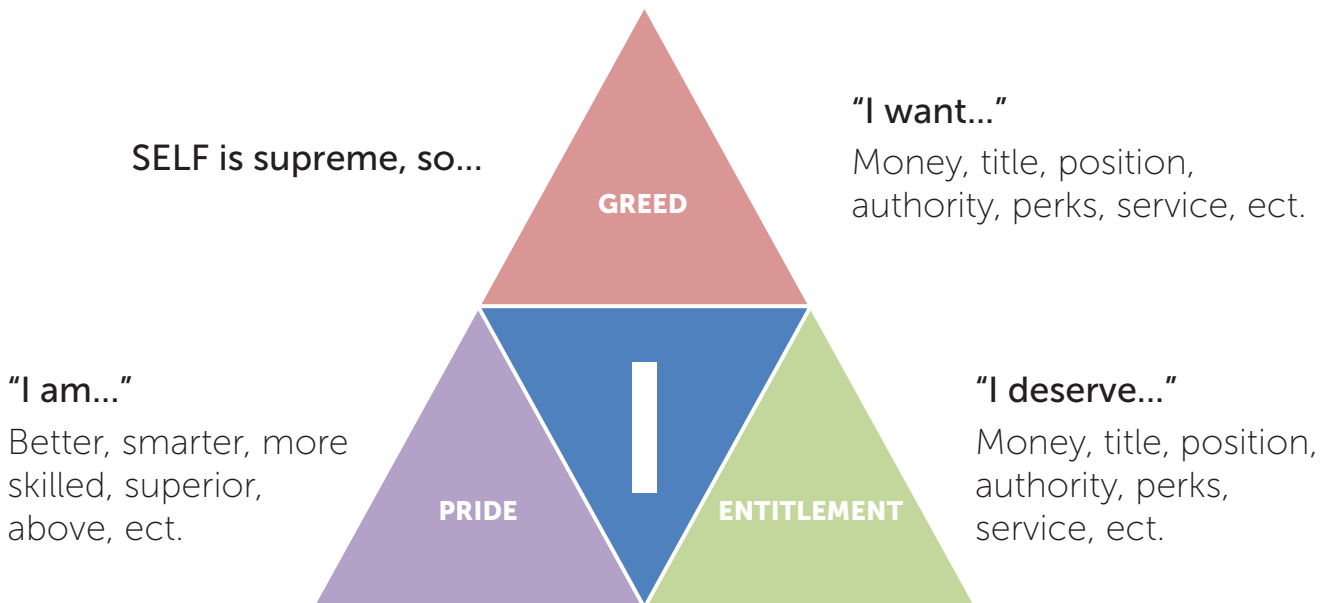
The Executive Fraud Triangle

Certified Fraud Examiner, Laura Downing built upon Cressey's original fraud triangle to develop an Executive Fraud Triangle (Figure 2), proffering that executives, and those in positions of power, have the ability to misuse that power and authority with limited challenge in order to benefit themselves or others.



Credit: Anders CPAs + Advisors: The Fraud Triangle: Three conditions that increase the risk of fraud
Figure 1: Cressey's Fraud Triangle

The Executive Fraud Triangle



Credit: Laura Downing. Fraud Magazine: The Executive Fraud Triangle: The great "I"
Figure 2: Downing's Executive Fraud Triangle

APPENDIX 2 - EXAMPLES OF FRAUDULENT AND CORRUPT CONDUCT

Forms of corruption

- **Bribery:** The offering, giving, receiving, or soliciting of something of value for the purpose of influencing the action of an official in the discharge of his or her public or legal duties
- **Embezzlement:** The fraudulent conversion of another's property by a person who is in a position of trust, such as an agent or employee
- **Extortion:** The obtaining of property from another induced by wrongful use of actual or threatened force, violence, or fear, or under colour of official right
- **Abuse of power:** Improper use of authority by someone who has that authority because he or she holds a public office
- **Abuse of privileged information:** Using information an employee has work related access to in order to benefit someone else
- **Favouritism:** the practice of giving special treatment to a person or group
- **Nepotism:** favouritism shown to relatives or close friends by those with power or influence
- **Patronage:** granting favours, giving contracts or making appointments to office in return for support
- **Theft:** the dishonest taking of property belonging to another person with the intention of depriving the owner permanently of its possession
- **Noble cause corruption:** utilisation of unethical, and sometimes illegal, means to obtain a desired result (the ends justifies the means)

Identifying what makes conduct corrupt rather than simply unlawful or unethical is difficult. Corrupt conduct may involve a crime, but not always. A person could act lawfully, but corruptly. A person's intention in acting in a particular way is relevant, but is not always the final factor in deciding if conduct were corrupt⁹.

Profits and benefits do not need to be of a high value. They may include: money, drugs, sexual favours or any other items. Advantages or favours may be for self or other people or groups.

- Conduct that uses proper powers and discretions for an improper purpose:
 - misusing legitimate authority to apply discretion such as:
 - 'turning a blind eye' to the criminal actions of friends, family or criminal associates
 - punishing or investigating other people without adequate cause
 - favouritism in the discharge of duties (for example issuing fines or other penalties to one group, but not to another)
 - misusing detention powers, such as unwarranted arrest or misuse of bail procedures
 - misusing surveillance, telephone interception or search powers
 - knowingly providing incorrect information in an affidavit to obtain access to intrusive powers
 - using powers to blackmail, extort or threaten individuals or organisations
 - excessive use of force (or threats) with a purpose to elicit information or prevent information from coming forward
 - using privileged access to information for personal purposes

⁹ What is law enforcement corruption? ACLEI Submission: Inquiry into the adequacy of aviation and maritime security measures to combat serious and organised crime (November 2009)

- Conduct that uses law enforcement functions to support or assist criminal activity:
 - participating in criminal activity, including using agency property, for example vehicles, uniforms, firearms or surveillance devices
 - offering or providing protection to criminal activity
 - offering or providing information to one or more criminal groups
 - engaging in any activity that sabotages law enforcement efforts
 - diverting law enforcement efforts or attention to, or away from, an activity in order to advantage one criminal group over another
 - using poor investigation practices to evade scrutiny of criminal activity
- Conduct that misuses information to support or assist criminal activity:
 - seeking or obtaining classified, sensitive, confidential or personal information, for any improper purpose
 - improperly seeking or obtaining information about law enforcement investigations, methods, processes or plans
 - providing or leaking information to unauthorised persons about individuals, witnesses, investigations or any aspect of law enforcement (including ‘backroom’ information not directly related to an investigation)
 - providing or leaking information to unauthorised persons that may assist them in a criminal act or that may advantage one criminal group over another
 - making unauthorised public comments about law enforcement methods, practices or targets
The term ‘information’ may include:
 - the personal or financial affairs of a colleague or law enforcement employee
 - witnesses, informers or anyone connected with an investigation or prosecution
 - criminal intelligence
 - assumed identities
 - detection or investigation methods
 - criminal methods
 - planned law enforcement actions or investigations (for example, ‘tip-offs’ about a pending execution of search warrants or a timetable for regulatory inspections or interdictions)
 - information technology or computer databases (that may assist hackers)
 - anything else that could provide an advantage to criminal activity
- Conduct that sabotages the impartial detection, investigation and prosecution of crimes:
 - agreeing to ‘look the other way’ when crime is committed
 - interfering with evidence, including failure to collect or document evidence properly
 - planting, falsifying evidence or ‘verballing’ to get a conviction or to ‘frame’ a person
 - destroying evidence which could incriminate a suspect or clear another
 - withholding criminal intelligence or information from an investigation
 - laying false charges, not laying charges or laying lesser charges
 - committing perjury
 - interfering with witness testimony or prosecution processes using bribery, extortion, blackmail or other promise, threat or inducement

- Leaking information about individuals engaged in investigations, joint operations, taskforces, etc.
- 'Grooming' or introducing others to corruption opportunities
- Forging qualifications or references to get a job or help place a person in an agency
- Favouritism or nepotism in recruitment, promotion or transfer
- Employment of family members, or influencing the recruitment or appointment of family members
- Passing on information about recruitment or promotion practices
- Improperly associating with criminals
- Engaging in criminal or suspect activity, such as illicit drug-taking or heavy
- Gambling
- Using the uniform to support private business, for example, to imply law enforcement support for a questionable activity
- Selling of work issued uniforms or equipment
- Using a police vehicle, firearm or other law enforcement-related property for private or illegitimate purposes.
- Failure to declare conflicts of interest or improper associations
- Failure of supervisor to manage or treat conflicts of interest raised or declared by staff
- Accepting a 'share' of profit or benefits from others' corrupt activities
- Failing to report corrupt activity or misconduct
- Attempting to cover up or hide misconduct or corrupt behaviour of self or others
- Obstructing inquiries of the Internal Affairs Unit, Professional Standards, the Corruption and Crime Commission and other government or regulatory bodies
- Using WA Police Force resources, including work-time, to conduct secondary employment. This includes conducting secondary employment while on sick leave
- Amending or falsifying medical certificates in order to obtain sick leave
- Taking sick leave when not sick
- Supplying information obtained from a restricted access database to an unauthorised person
- Disclosing official secrets or information to a third party
- Misappropriating grant funds
- Falsifying or fabricating research/review/evaluation outcomes
- Submitting a record of attendance containing false information or times not worked
- A manager signing off on fraudulent overtime claims
- Stealing money, property or drugs during arrests, execution of search warrants or other contact with the public
- Theft and skimming (e.g. removing and selling inventory, cash, consumables, or information, fraudulent acceptance of goods and services, and receiving compensation without reporting transactions)
- Regularly taking resources, such as office supplies, stationery or WA Police Force equipment, home for personal use or to sell for personal benefit

- Unauthorised use of a WA Police Force motor vehicle
- Approving invoices for private expenses or colluding to do so for others
- Requesting service staff change item names on bills and receipts when paying by corporate credit card. For example, requesting alcohol be recorded as a food item
- Submitting a false travel or reimbursement claim and receiving a benefit to which they are not entitled
- Misusing taxi vouchers for personal use or profit
- Payroll fraud (e.g. adding fake employees to the payroll or claiming overtime for hours not worked)
- Manipulating recruitment and selection procedures to secure the appointment of a close friend or family member or associate. This includes higher ranked individuals 'suggesting' outcomes to lower ranked individuals (power disparity)
- Management promoting, engaging or giving an employee advantage over others for personal reasons
- Failing to declare a conflict of interest but continuing to deal with a close associate in exercising a public duty (for example, recruitment or promotion processes)
- Accepting or soliciting a bribe or secret commission from a tenderer to give consideration to them
- Inappropriate relationships between procurement officers and suppliers
- Corruption in responding to errors or problems in the delivery of services
- Misuse of public resources (ICT equipment, phones, vehicles and equipment) for private use
- Providing commercial-in-confidence information to a tenderer resulting in them obtaining an unfair advantage over other tenderers in the tender process.
- Colluding with a supplier of goods or services to the WA Police Force for personal gain
- Facilitation payments i.e. obtaining kickbacks for organising preferential treatment
- Gifts or entertainment received which is intended to achieve a specific or generic WA Police Force outcome in the short or long-term

APPENDIX 3 - RED FLAGS OF FRAUDULENT AND CORRUPT CONDUCT ¹⁰

The following is an abbreviated list (not comprehensive), and are only indicators.

Opportunity Red Flags: Employees Against the Company

- Familiarity with operations and in a position of trust
- Close association with suppliers and other key people
- The firm that does not inform employees about rules or of the action taken to combat fraud
- Rapid turnover of key employees
- No mandatory vacations, or periodic rotations etc
- Inadequate personnel screening policies when hiring employees to fill positions of trust
- Absence of explicit and uniform personnel policies
- No maintenance of accurate personnel records of dishonest actions and disciplinary actions
- Executive disclosures and examinations not required
- Dishonest or overly dominant management
- Operating on a crisis mode
- No attention to details
- Unrealistic productivity measurements
- Poor compensation practices
- Lack of internal security
- Inadequate training programs

Opportunity Red Flags: Individuals on Behalf of the Company

- Related-party transactions
- Complex business structure
- Ineffective internal audit staff
- Highly computerized company
- In atypical or “hot” industries
- Uses several audit firms or changes auditors frequently
- Reluctant to provide auditors with needed data
- Uses several legal firms or changes firms often
- Uses an unusually large number of banks
- Continuous regulatory problems
- Large year-end or unusual transactions
- Inadequate internal control
- Unusually liberal accounting practices
- Poor accounting records
- Inadequate accounting staff
- Inadequate disclosure of unusual accounting practices

¹⁰Romney, M. B., W. S. Albrecht and D. J. Cherrington. 1980. Red-flagging the white collar criminal. Management Accounting (March): 51-54, 57.

Personal Characteristic Red Flags

- Rationalization of contradictory behaviour
- Lack of strong code of personal ethics
- A “wheeler dealer” personality
- Lack of stability
- A strong desire to beat the system
- A criminal or questionable background
- A poor credit rating and financial status

Situational Pressure Red Flags: Employees Against the Company

- High personal debts or financial losses
- Inadequate income for lifestyle
- Extensive stock market or other speculation
- Excessive gambling
- Undue family, company or community expectations
- Perceived inequities in the organization
- Resentment of superiors and frustration with job
- Peer group pressures
- Undue desire for self-enrichment and personal gain

Situational Pressure Red Flags: Management on Behalf of the Company

- Unfavourable economic conditions within the industry
- Insufficient working capital or high debt
- Dependence on one or two products, customers or transactions
- Severe obsolescence
- Extreme rapid expansion through new business or product lines
- Reduced ability to acquire credit, or restrictive loan agreements
- Cost and expenses rising faster than revenues
- Difficulty collecting receivables
- Progressive deterioration in quality of earnings
- Significant tax adjustments
- Urgent need for favourable earnings to support high price of stock or to meet earnings forecast
- Need to gloss over a temporary bad situation to maintain management prestige
- Significant litigation, especially between stockholders and management
- Unmarketable collateral
- Significant reduction in sales backlogs
- Possibility of license being revoked
- Suspension or delisting from a stock exchange
- Pressure to merge
- Sizable inventory increase without comparable increase in sales

Disclaimer: The information contained in this publication is provided in good faith and believed to be accurate at time of publication. The State shall in no way be liable for any loss sustained or incurred by anyone relying on the information.
Revised edition March 2022