Fraud and Corruption Control Framework

2023

Contents

1. Clear Expectations

CIT Board

The Board of the Canberra Institute of Technology (CIT)

2. Terms and Definitions

The CIT Fraud and Corruption Framework is intended to align with the *Australian Standard for Fraud and Corruption Control AS 8001:2008*, and adopts the same definitions as outlined in the Standard. It is noted that the ACT Government also maintains an ACTPS Integrity Framework, which contains unique definitions. Where there is a conflict, the Australian Standards definitions apply, with a notation of the ACTPS Integrity Framework definition.

Terms and Definitions

Attack – an attempt to destroy, expose alter, disable, steal or gain unauthorised access to, or make unauthorised use of, an asset.

Bona fide/bona fides – a person or organisation whose business practices appear to be straightforward and conducted with integrity.

Bribe/bribery – offering, promising, giving, accepting or soliciting 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.

Note 1 to entry: the above is a generic definition. The meaning of the term bribery is as defined by the antibribery law applicable to CIT and by the anti-bribery management system designed by CIT.

Business associate – external party with whom CIT has, or plans to establish, some form of business relationship.

Note 1 to entry: A business associate includes but is not limited to clients, customers, joint ventures, joint venture partners, consortium partners, outsourcing providers, contractors, consultants, sub-

Note 1 to entry: Control include any process, policy, device or practice, or other actions which modify risk.

Note 2 to entry: Controls may not always exert the intended or assumed modifying effect.

Corruption – dishonest activity in which a person associated with CIT (e.g., director, executive, manager, employee or contractor) acts contrary to the interests of CIT 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 CIT, or a person purporting to act on behalf of and in the interests of CIT, to secure some form of improper advantage for the organisation, either directly or indirectly.

Note 1 to entry: the concept of corruption in this framework is broader than the concept of bribe or bribery in AS ISO 37001. All acts of bribery would constitute corruption under this framework but not all acts of corruption would constitute bribery under AS ISO 37001.

Note 2 to entry: while conduct must be dishonest for it to meet the definition of corruption, the conduct does not necessarily represent a breach of the law.

Cybercrime – criminal activity, where services or applications in the cyberspace are used for or are the target of a crime, or where the cyberspace is the source, tool, target or place of a crime.

Digital evidence – information or data, stored or transmitted in binary form that may be relied on as evidence.

Digital evidence first responder/DEFR – individual who is authorised, trained and qualified to act first at incident scene in performing digital evidence collection and acquisition with the responsibility for handling that evidence.

Note 1 to entry: Authority, training and qualifications are the expected requirements necessary to produce reliable digital evidence, but individual circumstances may result in an individual not adhering to all three requirements. In this case, the local law, CIT policy and individual circumstance should be considered.

External fraud/externally investigated fraud – fraudulent activity where no perpetrator is employed by, or has a close association with, the target organisation.

Fraud – 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.

Note 1 to entry: Property in this context also includes intellectual property and all other tangibles such as information.

Note 2 to entry: 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 financial benefit.

Note 3 to entry: 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.

Investigation – search for evidence connecting or tending to connect a person (either natural person or a body corporate), with conduct defined by this framework as fraud or corruption.

Management system – set of related, or interacting elements, of an organisation to establish policies and objectives, and processes to achieve those objectives.

Note 1 to entry: A management system can address a single discipline or several disciplines.

3.

CIT Fraud and Corruption Prevention Plan

Part 2.3 of the Public Sector Management Standards 2006 requires all ACT Government organisations, (including CIT) to develop and implement a Fraud and Corruption Prevention Plan (the Plan). This plan must be developed in conjunction with relevant strategic risk assessments. Under the CIT Fraud and Corruption Framework, the Plan is the key reference for planning and implementing fraud and corruption prevention activities. The Plan must be reviewed every two years.

The following matters must be contained, or as appropriate considered as part of the Plan:

- The Plan should be based upon a recent fraud and corruption risk assessment and will deal with those risks in priority order.

- While risk management standards allow for several responses for dealing with risks – including accepting risks, insuring against risks, and sharing risks – these responses are not appropriate when dealing with integrity. CIT integrity risks should be dealt with by improving controls and raising employee awareness.

- The Plan must clearly identify which CIT line area is responsible for dealing with the fraud and corruption risk.

The Plan must include a description of the CIT SERBIR's role, which includes the requirement to:

- monitor and ensure the Plan is implemented

- coordinate any risk treatments that involve more than one area of the CIT.

- The Plan should contain a realistic timetable for implementation. It should reflect the priority of and potential consequences of the risk in the risk assessment process.

- The Plan should outline how responses to integrity risks will be coordinated with other governance mechanisms including internal audit, physical security and IT security.

The CIT CEO must implement strategies in the Plan to actively detect potential weaknesses or exposures to fraud and corruption risks within CIT's programs and operations, in accordance with privacy and budget considerations.

The CIT CEO must ensure that the Plan and the integrity arrangements in CIT are assessed and reviewed every two years, or more frequently, if:

any significant suspected fraud or corruption is discovered; or

there is a significant change in the nature or scope of operations, procedures or systems.

- a review of the Plan is required,

The fraud

organisational disruption

loss of employment

financial and operational performance

ability to attract and retain capable staff

ability to raise capital and impact on credit rating

impact on third parties.

CIT will apply the risk management principles set out in ISO 31000:2018 (Risk Management Guidelines) in the management of fraud and corruption risk and, in doing so, will apply the six-stage risk management process in accordance with ISO 31000:2018 comprising the following:

communication and consultation

scope, context, and criteria

risk assessment

risk treatment

monitoring and review

recording and reporting.

In applying the ISO 31000:2018 risk management principles, framework and process, CIT will consider the additional guidance included in the following risk assessment handbooks:

SA HB, delivering assurance based on ISO 31000:2018

SA/SNZ HB 89 Risk Management – Guidelines on Risk assessment techniques

SA/SNZ HB 436 Risk management guidelines – companion to AS ISO 31000.

‘PESTLE” model for external environment scan

Political environment	To identify the political situation of a country in which CIT operates, including the stability and leadership of the government, whether there is a budget deficit or surplus, lobbying interests and international political pressure.
Economic environment	To determine the economic factors that could have an impact on CIT, including interest rates, inflation, unemployment rates, foreign exchange rates and monetary or fiscal policies.
Social Environment	To identify the expectations of society by analysing factors such as consumer demographics, significant world events, integrity issues, cultural, ethnic and religious factors, and consumer opinions.
Technological environment	To identify how technology, including technological advancements, social media platforms and the role of the internet more broadly, is affecting or could affect CIT.
Legal environment	To identify how specific legislation, including industry specific legislation, and case law are affecting or could affect CIT’s future operations.
Environmental factors	To identify how national and international environmental issues are affecting or could affect CIT.

In conducting external environmental scanning, CIT will monitor the following:

ASQA regulatory compliance aspects

newspapers

news sites

websites

social media platforms

blogs

podcasts

industry journals

magazines

books

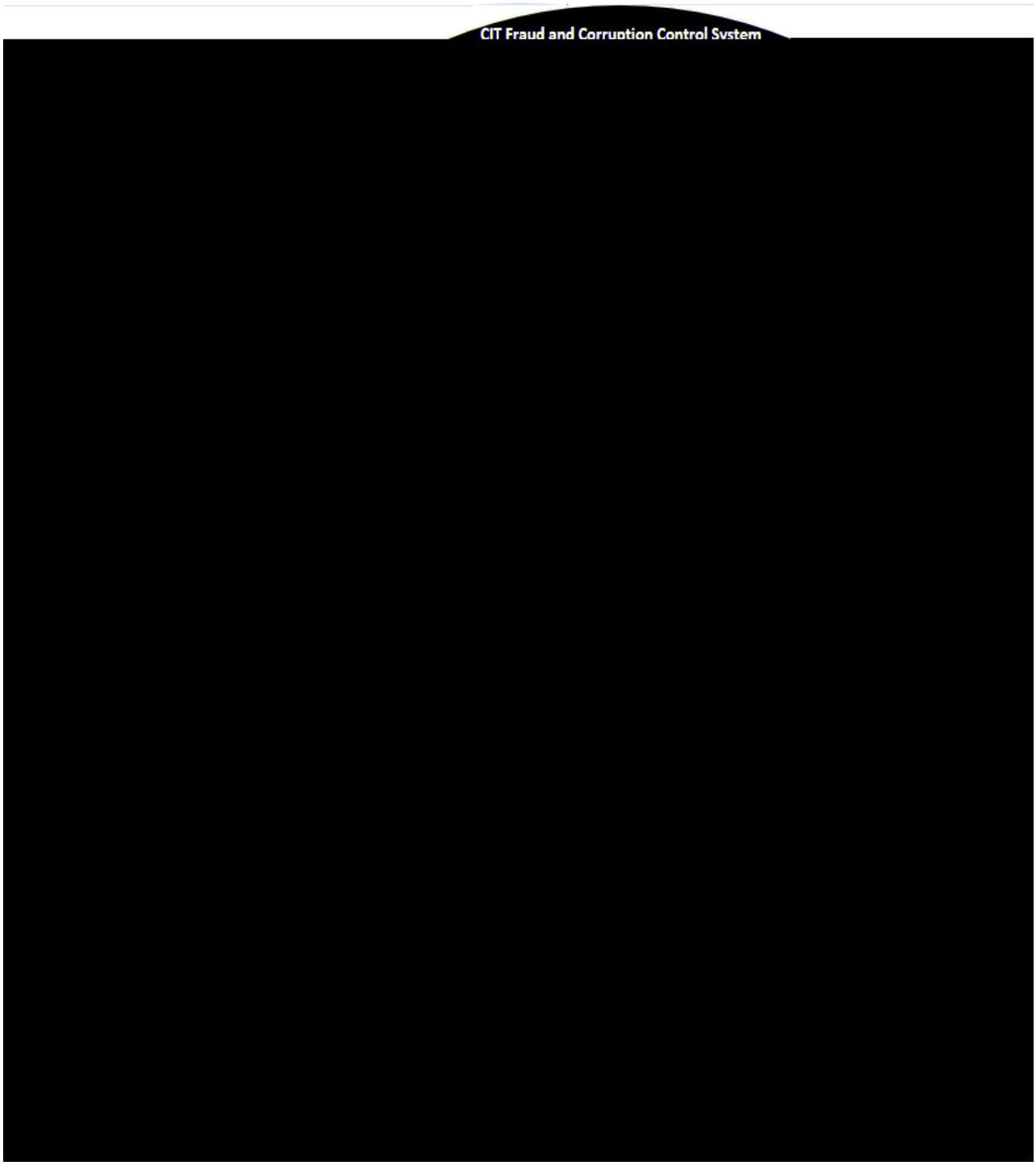
reports e.g., World Economic Global Risk Report

surveys

interviews

p

CIT Fraud and Corruption Control



Promoting the fraud and corruption control system

CIT will effectively communicate and promote the FCCF internally and, where appropriate, externally. It is important CIT's workforce is aware of:

- the indicators of fraud and corruption
- what is expected of them when they identify or suspect fraud or corruption
- what action will be taken about reported fraud and corruption.

Relevant elements of CIT's FCCF should be communicated to all interested external parties through:

- an appropriate note to CIT's Annual Report as part of a general declaration of integrity or corporate governance
- a declaration, in a request for tender or via terms and conditions when undertaking business with external parties
- CIT's website.

Monitoring and maintaining a fraud and corruption control system

A program for monitoring the implementation, operation and maintenance of the FCCF will be established, including key milestones and resourcing requirements.

The purpose of such a program is to ensure the FCCF:

- addresses the objectives for which the system was created
- is 'fit for purpose' in terms of the organisation's fraud and corruption control needs
- has been updated in light of any changes in CITs operations and/or risk assessment since the last review.

4.

Element Custodian Responsibility Status	Element Custodian Responsibility Status	Element Custodian Responsibility Status
Legislation and regulations	Board, SERBIR, all Executive Directors, Audit and Risk Committee and EBM Audit, Risk and Corporate Governance and all staff and contractors.	See - Section 5 Legislation, regulations and policy.
Risk analysis and planning for integrity	CIT Board, SERBIR, all Executive Directors, Audit and Risk Committee, EBM Audit, Risk and Corporate Governance and risk owners.	Responsible for conducting a fraud risk assessment every two years.
Internal controls, audit and governance	CIT Board, SERBIR, all Executive Directors, Audit and Risk Committee, EBM Audit, Risk and Corporate and risk owners.	The Audit and Risk Committee is responsible for monitoring and reviewing the effectiveness of corporate governance mechanisms within directorates and agencies. A function of the Audit and Risk Committee is to provide an independent opinion to the CEO regarding the adequacy of risk management processes. To perform this function, the SERBIR will need to provide the Audit and Risk Committee with integrity-related risk assessments for CIT, proposed strategies to address risks, and action being taken to address unacceptable risk levels. The Audit and Risk Committee may arrange for independent reviews of any of the management processes regarding risk

5. Legislation, standards, frameworks and policies

The table below describes the legislation, standards, frameworks and policies relating to the FCCF.

Legislation, standards, Policy or Framework	Description of obligation

any changes to procedures and practices arising from the incident.
The Audit and Risk Committee should have access to regular reports of information from the fraud and corruption reporting system.

	placed on the head of the directorate to manage the directorate in accordance with the Act.
CIT Finance Policy	This document outlines the processes to be followed for financial transactions to achieve consistency, accuracy and transparency and to manage financial risk. The policy provides links to associated policies which underpin and complement the Finance Policy.
CIT Risk Management Policy and Procedure	This policy applies to all CIT employees, activities, students, contractors, and visitors. The CEO, CIT Board, CIT Audit and Risk Committee and all CIT staff are to use the risk management methodology outlined in these documents to manage CIT fraud, corruption and integrity risks.
ACT Public Service Code of Conduct 2022	All CIT employees must: • exercise authority in accordance with the stated values and principles of the ACTPS and the control of fraud and corruption; • be apolitical, honest, dependable, and accountable when dealing with Ministers, the Legislative Assembly, the public and colleagues; • respond appropriately in difficult situations; • recognise achievement; • do not shirk from uncomfortable conversations; • take responsibility and are accountable for their decisions and actions and are consistent when dealing with others; and • engage genuinely with the community, and manage the resources entrusted to them honestly and responsibly.
Public Interest Disclosure (Integrity Commission – Managing Disclosures and Conducting Investigations) Guidelines 2021	CIT is required to collect sufficient information about its disclosure officers, and make it readily available, to ensure potential reporters can easily make disclosures, and select officers they would feel most comfortable making their disclosure to. This would require, at a minimum, the collection of the nominated disclosure officer's: • name • role • work location • phone number (i.e., their desk/office number) • email address • postal address As CIT does not have a case management system that can be adapted for activities under the PID Act, the Commission recommends the use of the ACT Government's document management system (TRIM in the case of CIT). s20(1) of the PID Act provides that CIT must investigate all disclosures which CIT receives, and that such investigations must comply with the rules of natural justice and procedural fairness. s23 of the PID Act requires CIT as an investigating entity to keep the discloser informed about the status of any investigation at least once every three months.

6. Internal controls, audit and governance

In line with AS/NZS ISO 31000:2018 (Risk Management Guidelines) a CIT audit plan must be developed to focus on risks identified as being ‘extreme’, ‘high’ or those

7. Fraud and corruption detection systems

Despite having implemented fraud and corruption prevention controls, it is possible that fraud and corruption may occur from time to time.

The following elements, discussed further below, form part of CIT's detection regime:

All CIT staff are responsible for developing and maintaining appropriate detection strategies to mitigate the risk of fraud and corruption. Detection strategies should be aimed at identifying fraud and corruption as soon as possible after it has occurred, in the event that preventative systems fail. Fraud and corruption and detection are to be addressed and applied by the FCCP.

Fraud and corruption detection may be achieved through:

- enhancement of fraud awareness and reporting responsibilities amongst CIT's employees (refer to Fraud and Corruption Awareness Training and Reporting of Fraud and Corruption)
- vigilance on the part of line management, who must be aware of their responsibility to identify and report any suspected or actual fraud or corruption activity
- data analysis activities and exception reporting using electronic data
- maintaining and monitoring audit trails
- development of specific detection strategies for action by line management
- periodic management reviews instigated by CIT's management team.

It is incumbent on all CIT staff members to be alert to the potential for fraud and corruption to take active steps to detect any fraud and corruption that occurs. The SERBIR will assist line management coordinate the development and maintenance of systems and procedures to detect fraud and corruption (as specified above).

8. Ongoing improvement

Ongoing improvement for fraud and corruption prevention is primarily achieved via the Fraud and Corruption Prevention Plan review process. This review process includes review of:

- fraud and corruption risk assessment
- measures of performance and effectiveness of detection strategies
- risk mitigation strategies
- lessons learned from the previous Fraud and Corruption Prevention Plan
- input from liaison with other SERBIRs/Directorates and the ACT Integrity Commission.

9. Model and embody a culture of integrity

The CIT Executive (top management) is ultimately responsible for building and maintaining an organisational and staff culture, based on integrity, to mitigate instances of misconduct and corruption.

Values and standards

All of CIT's mission, vision and values statements will include references to integrity and the code of conduct (and other references), which set the standard of behaviour at CIT./P ᚴ

10. Learn and develop integrity knowledge and skills

CIT Human Resources will integrate and embed integrity aspects into all training and education strategies, plans and services provided to CIT staff (including the CIT Strategic Workforce Plan, noting the specialist fraud and corruption resources required to support this framework detailed previously above).

CIT Human Resources will ensure all staff are immersed with integrity awareness and training from recruitment through to separation of employment from CIT.

Integrity education and capacity

CIT managers will provide and integrate integrity awareness training aspects into all: staff performance processes

staff training plans

division, branch and section work plans/ operational plans

mentoring and/or networking programs and opportunities

pathways where staff can seek integrity advice and guidance (if not from their direct supervisor).

11. Be accountable for integrity

All CIT staff are responsible for acting with integrity, noting the ultimate responsibility for staff and organisational integrity rests with the CIT CEO.

ACT Reportable Conduct (for CIT Employees or volunteers)

CIT must report allegations or convictions made against CIT employees or volunteers that occurred after **1 July 2017** to the Ombudsman.

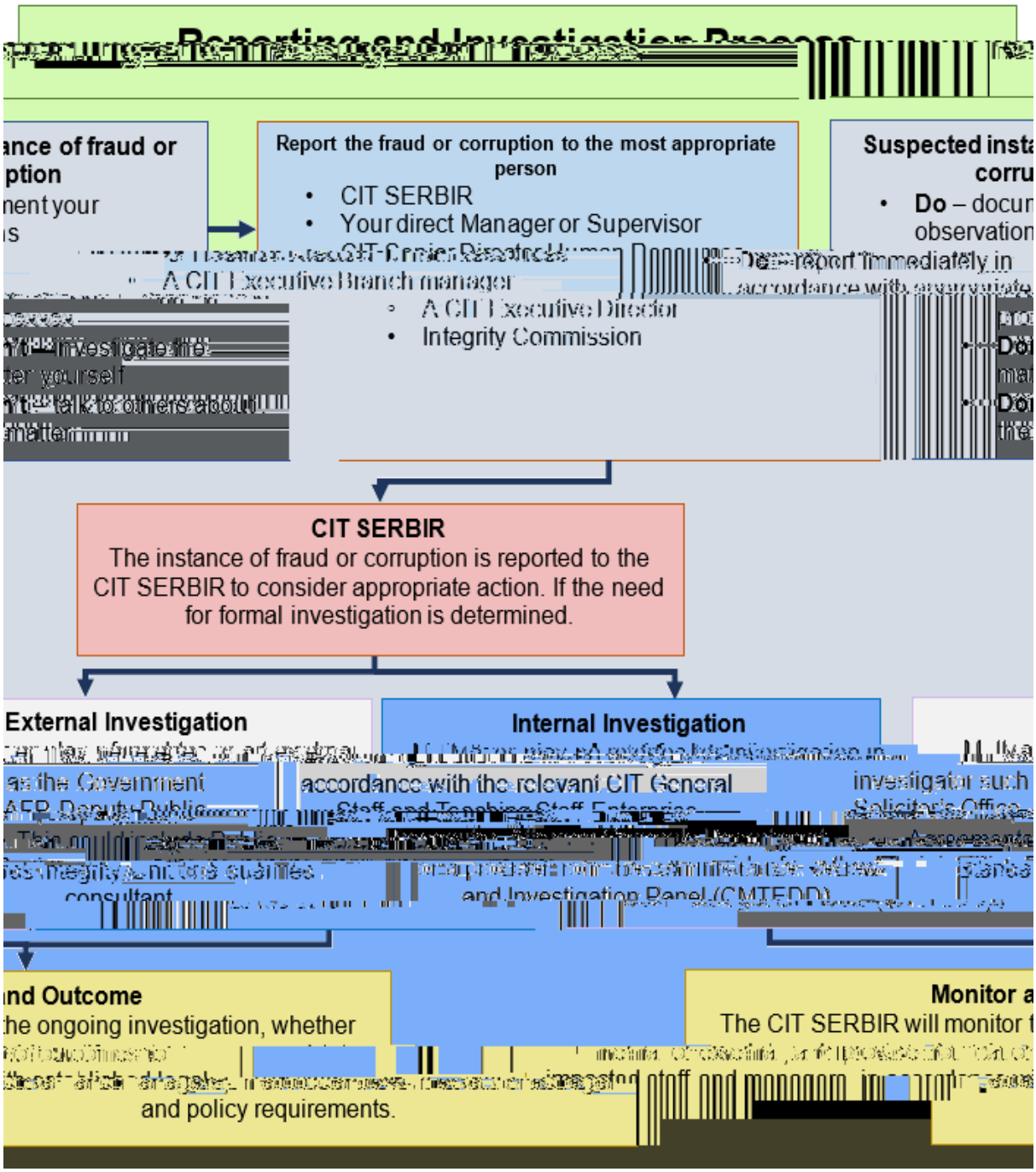
CIT must:

- notify the Ombudsman within **30 days** of becoming aware of the allegation by completing the section 17G notification form
- provide details of the allegation or conviction
- provide CIT's intended response, including an investigation plan and risk assessment
- report to appropriate organisations. These may include ACT Policing, Child Youth Protection Services and Access Canberra (Working with Vulnerable People).

Refer also to Reporting and Investigation Process enclosed further below

ACT Reportable Conduct for the ACT Community (including students)

Memby t2.3 (p- (b-3 di)-3.7 (nc)O1-3 di)G non-12.3 (at)-1.1 (i)-8.9 (on)-12.2 (P)2.4 (r)-6.4 (oc)-8 (es
Yout tud1 (r)7 (ot)12 (ec)4 (t 3 (at)-1.1 8h(c)4 (o)1d)-12.2 (2d( )(es)3.9w 8.8T



Outcomes of any reporting and investigation activities are to be considered in the review of the Fraud and Corruption Control Plan as lessons learnt.

12. Self-analysis and review

This Framework will be reviewed in parallel with the Fraud and Corruption Prevention Plan (at least every two years). This Framework will take into any factors that emerge from the review of the Fraud and Corruption Prevention Plan (specifically the risk assessments, performance measurement lessons learnt) elements) and incorporate these into a revised Framework where required. _

13. Oversight

The oversight of fraud and corruption activities and integrity aspects more broadly is detailed in Section 4 -