Canberra Institute of Technology

RTO Code 0101 | CRICOS No. 00001K

Fraud and Corruption Control Framework

2023

Contents

1. Clear Expectations

CIT Board

The Board of the Canberra Institute of Technology (CIT) does not tolerate any level of fraud or corruption, and views fraud and corruption as serious offences. The CIT Board is committed to the integrity of the organisation and a comprehensive and systematic approach to the effective management of fraud and corruption risks and vulnerabilities.

In July 2023, the CIT Board issued a Fraud and Corruption Policy to protect the assets and reputation of CIT. The policy outlines the definitions of fraud and corruption and clearly articulates the responsibilities of all CIT staff, including the CEO, executives, officers, and contractors. Preventing and controlling fraud and corruption is everyone's responsibility.

The CIT Audit and Risk Committee, a subcommittee of the CIT Board, provides independent, objective assurance and assistance to the CIT Board on CIT's risks, control and compliance framework and has responsibility for maintaining the integrity of CIT. This is done by ensuring CIT has appropriate processes and systems in place to detect, capture and effectively investigate fraud and corruption information and by receiving regular updates on any matters before the Senior Executive Responsible for Business Integrity Risks.

Effective measures to prevent fraud and corruption are critical in ensuring that CIT provides the highest standard of client services, across all teaching, learning and business areas, and maintains public confidence in its operations.

The CIT Fraud and Corruption Control Framework identifies the objectives, policies and strategies to minimise the opportunities for fraud and corruption to occur in the CIT environment and provides CIT staff with the right information and tools to deal with matters of fraud and corruption that may present.

CIT Chief Executive Officer

As the Chief Executive Officer of the Canberra Institute of Technology, I am committed to ensuring CIT staff operate with the highest level of integrity and accountability and demonstrate the standard of behaviours and expectations as set out in the ACT Public Service Code of Conduct. As a government agency, it is imperative the public trust in our organisation, and that we deliver high-quality, efficient and effective programs and services.

The CIT Fraud and Corruption Framework is an essential component of CIT's governance arrangements. The Framework provides guidance and directions for employees and students on how to identify and prevent fraudulent and corrupt activities.

The Framework is based on a thorough assessment of our fraud and corruption risks, and describes the instruments, structures and cultural factors that guide how we practice, manage and account for integrity. While it identifies officers with particular roles, all CIT employees (including CIT teaching staff) and CIT students are responsible for promoting integrity and preventing misconduct, including fraud and corruption, through their daily activities. CIT has zero tolerance for actions that compromise our integrity or enable corrupt and fraudulent behaviour.

Through the CIT Executive and Senior Executive Responsible for Business Integrity Risk (SERBIR), I commit to monitoring and maintaining this Framework, reviewing its effectiveness and seeking assurance from across CIT that our approach to integrity is sound.

I want to be clear that we all have responsibility for safeguarding the integrity of CIT and preventing misconduct and corruption. We demonstrate this, in part, by reporting any integrity breaches we see or become aware of, and making suggestions on how we can improve our approach to integrity.

As CIT employees and students, I expect you to familiarise yourself with this Framework.

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-contractors, suppliers, vendors, advisors, agents, distributors, representatives, intermediaries and investors. This definition is deliberately broad and should be interpreted in line with the bribery risk profile of CIT to apply to business associates which can reasonably expose the organisation to bribery risks.

Note 2 to entry: Different types of business associate pose different types and degrees of bribery risk, and CIT has different degrees of ability to influence different types of business associate. Different types of business associate can be treated differently by CIT's bribery risk assessment and bribery risk management procedures.

Note 3 to entry: Reference to "business" in this document can be interpreted broadly to mean those activities that are relevant to the purposes if CIT's existence.

Code of behaviour/code of conduct/code of ethics – a document broadly communicated within CIT, setting out expected standards of behaviour.

Conflict of interest – a situation where business, financial, family, political or personal interests could interfere with the judgement of persons in performing their duties for the organisation.

Control – a measure that is modifying a risk.

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.

Note 4 to entry: The concept of fraud within the meaning of this framework can involve fraudulent conduct by internal and/or external parties targeting CIT or fraudulent or corrupt conduct by CIT itself targeting external parties.

Fraud and corruption control framework/FCCF – framework for controlling the risks of fraud and corruption against or by CIT.

Note 1 to entry: This is also referred to as a fraud and corruption control framework (FCCF).

Fraud and corruption event – instance of fraudulent or corrupt activity against or by CIT.

Fraud and corruption risk assessment – application of risk management principles and techniques to assess the risk of fraud and corruption within an organisation in accordance with AS ISO 31000.

Governing body – group or body that has ultimate responsibility and authority for CIT's activities, governance and policies, and to which top management reports and by which top management is held accountable.

Note 1 to entry: Not all organisations, particularly small organisations, will have a governing body separate from top management.

Note 2 to entry: A governing body can include, but is not limited to, board of directors, committees of the board, supervisory board, trustees or overseers.

Information security – preservation of confidentiality, integrity and availability of information.

Note 1 to entry: In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

Information security management system – part of the overall management system, based on a business risk approach, which establishes, implements, operates, monitors, reviews, maintains and improves information security.

Note 1 to entry: The management system includes CIT structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

Information security management system (ISMS) professional – person who establishes, implements, maintains and continuously improves one or more information security management system processes.

Interested party/stakeholder – person or organisation that can affect, be affected by or perceive itself to be affected by a decision or activity.

Internal fraud/internally investigated fraud – fraudulent activity, where at least one perpetrator is employed or has a close association with the target organisation and has detailed internal knowledge of the organisations operations systems and procedures.

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.

Note 2 to entry: The system elements may include the organisation's structure, roles and responsibilities, planning and operation.

Note 3 to entry: The scope of a management system may include the whole of the organisation, specific and identified functions of the organisation, specific and identified sections of the organisation, or one or more functions across a group of organisations.

Monitoring – determining the status of a system, a process or an activity.

Note 1 to entry: To determine the status, there may be a need to check, supervise or critically observe.

Organisation – the person, or group of people, that functions with responsibilities, authorities and relationships to achieve its objectives. CIT is defined as an organisation within this framework.

Note 1 to entry: The concept of organisation includes, but is not limited to, sole trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

Note 2 to entry: For organisations with more than one operating unit, one or more of the operating units can be defined as an organisation.

Policy – intentions and direction of an organisation, as formally expressed by its top management and governing body.

Preservation – process to maintain and safeguard the integrity and/or original condition of the potential digital evidence.

Reportable Conduct – covers allegations or convictions of child abuse or misconduct toward children. CIT must report allegations of reportable conduct by an employee or volunteer, including:

- ill-treatment of a child (such as emotional abuse or use of force)
- neglect
- psychological harm
- misconduct of a sexual nature
- sexual or physical offences and convictions where a child is a victim or is present

- inappropriate discipline or not protecting children from harm.

Risk – effect of uncertainty on objectives.

Note 1 to entry: An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats.

Note 2 to entry: Objectives can have different aspects and categories and can be applied at different levels.

Note 3 to entry: Risk is usually expressed in terms of risk sources, potential events, their consequences and their likelihood.

Risk assessment – overall process of risk identification, risk analysis and risk evaluation.

Serious risk – likely to have an impact on the organisation, if it occurred, with the potential to threaten the organisations' economic viability in the short, medium or long term, or to have a noticeable impact upon the organisations business reputation.

Target organisation – fraud against, or by, an organisation that relies heavily on information technology, and which would not be possible without information technologies.

Note 1 to entry: The concept of technology – enabled fraud types follow the binary classification of cyber- enabled and cyber-dependent crimes in which the former includes frauds made possible through the use of technologies, which the latter are so called 'pure' cybercrimes that require the presence of technologies for their commission- such as access and description offences.

Threat – potential cause of an unwanted incident, which can result in harm to a system or organisation.

Top management – person, or group of people, that directs and controls an organisation at the highest level.

Note 1 to entry: Top management has the power to delegate authority and provide resources within the organisation.

Whistle blower – person who reports a wrongdoing.

Note 1 to entry: Applicable whistle blower protection legislation may apply.

3. Plan and Act to Improve Integrity

This document outlines the framework by which fraud and corruption prevention will be integrated and managed across all CIT activities.

The CIT Fraud and Corruption Control Framework (the Framework) is underpinned by the ACTPS Integrity Framework (2022) and ACTPS Integrity Governance Policy (2022). The Framework provides further detail and guidance around the application of fraud and corruption control aspects as they relate to CIT as an ACT Government Territory Authority[1]. Together with the CIT Risk Management Framework, they facilitate the effective management of integrity-based risks.

Governing body

The CIT governing body has ultimate responsibility and authority for CIT's integrity activities, including fraud and corruption arrangements. The Audit and Risk Committee is a subcommittee of the CIT Board, which has been given responsibility for the oversight of risk, including fraud and corruption[2]. As such, the CIT Audit and Risk Committee, reporting to the CIT Board is responsible for oversight of CIT's:

- fraud and corruption control systems
- fraud and corruption risk assessments
- information security and Information security management systems (ISMSs)
- fraud and corruption policies
- fraud and corruption prevention plans
- resourcing, to ensure the operation and maintenance of the CIT Fraud and Corruption Control Framework.

The CIT Executive (including the CEO) is responsible for the day-to-day monitoring and implementation of these components. Changes that significantly impact any component of Framework must be agreed to by the Executive Management Committee prior to being presented to the CIT Audit and Risk Committee for their agreement.

In the event of an urgent change, to prevent an imminent or immerging threat, the CEO may implement a temporary change to address the threat. This will provide the Executive Management Committee and Audit and Risk Committee appropriate time to understand the nature of the situation and most appropriate resolution.

[1] See s5, *Canberra Institute of Technology Act* 1987 (ACT).
[2] See CIT Audit and Risk Committee Charter.

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, which will usually entail:
  - determining that the risk assessment methodologies are valid
  - conducting another risk assessment
  - reviewing changes in the programs, operation, and environment since the last Plan
  - prioritising any outstanding recommendations from the last fraud and corruption prevention audit that are yet to be implemented
  - developing a further two-year program for fraud and corruption prevention, which will rectify residual shortcomings in the procedures.

Note: if there has been a major change in the functions, responsibilities or procedures of the directorate/agency, a further risk assessment may need to be conducted and if new risks are identified, the plan should be altered accordingly. Machinery of Government changes may warrant a need for a risk assessment to be updated outside the usual cycle.

Specialist fraud and corruption control resourcing

The CIT governing body, through the CEO, must implement an appropriate level of fraud and corruption control resourcing based upon the organisation's assessed fraud and corruption exposures.

This includes the appointment of specialised fraud and corruption control personnel, as appropriate to CIT's assessed risk exposures, whose role includes:

- developing, implementing and maintaining CIT's FCCF
- coordinating periodic assessment of the organisation's fraud and corruption risks
- recording fraud and corruption events
- escalating and monitoring fraud and corruption events, including coordinating internal and external reporting
- conducting coordinating or monitoring investigations into allegations of fraud and corruption.

Fraud and corruption control resourcing may involve recruitment of specialist resources, internal or external to CIT, with the requisite skills and experience or, alternatively, training existing personnel in this role.

The fraud and corruption control function should ideally be no more than two levels removed from the CEO or, alternatively, directly report to the CEO on fraud and corruption control issues.

The person(s) appointed to these positions should have the capacity to understand and apply current better practice in fraud and corruption control, and the ability to coordinate and deliver awareness-raising on relevant fraud and corruption control procedures to:

- the governing body
- CIT Board through the CIT Audit and Risk Committee
- top management (CIT SES Band 1 employees and above)
- line management
- CIT employees.

CIT must ensure that a person delivering a specialist fraud and corruption control function remains up to date with best practice through:

- formal training on fraud and corruption control issues
- attendance at relevant seminars, conferences and workshops with a defined time commitment each year
- maintaining a library of reference materials
- networking with other fraud and corruption control specialists as part of a 'community of practice'.

Appointment of an CIT ISMS Professional

The CIT governing body, through the CEO, must ensure the management of technology-enabled fraud is undertaken by appropriately qualified information security resources. An ISMS professional shall have the following attributes:

- formal qualifications appropriate to the role of the ISMS professional
- sound understanding of the organisation's fraud and corruption exposures
- a program for continuing professional development in technology-enabled fraud and corruption
- a sound understanding of how an ISMS can effectively mitigate the risk of fraud and corruption

- a sound understanding of cybercrime and the methods for managing the risk of cybercrime as set out in ISO/IEC 27032:2012 (Information technology — Security techniques — Guidelines for cybersecurity).

Collaboration with other CIT risk management resources

The CIT governing body, through the CEO, must ensure fraud and corruption control initiatives are coordinated with CIT's broader risk management approach. The CIT specialist fraud and corruption resources (including the CIT ISMS professional) must closely collaborate with the other CIT risk management resources to ensure that fraud and corruption risks are incorporated into the overall CIT risk management system.

Leveraging organisational fraud and corruption control resources

A range of other CIT internal functions can be beneficial in the control of fraud and corruption. These internal functions include:

- human resources, industrial relations, payroll, complaints management and learning and development
- WHS personnel
- regulatory and compliance professionals
- facilities personnel (including physical and asset management)
- finance staff
- internal audit staff
- student services staff
- college and educational delivery staff
- policy staff
- communications staff.

These resources should be coordinated to control CIT's fraud and corruption exposures.

Line management

CIT must communicate to all line managers a mandatory accountability for promptly reporting fraud and corruption matters that come to their attention.

CIT must ensure line management personnel are fully aware that managing fraud and corruption is as much part their responsibility as managing other types of

enterprise risk. To reinforce this, it is important that CIT has a system in place containing the following elements:

- fraud and corruption is incorporated into the staff performance management system

- preventing and detecting fraud and corruption must be specified in the position description of all line managers where appropriate.

CIT business unit accountability for fraud and corruption control

Fraud and corruption control is sometimes seen as a high-level corporate issue in affected organisations, i.e., the responsibility for fraud and corruption control sits with top management rather than as a responsibility for local line management within business units that make up CIT.

Fraud and corruption events often occur in the business operations geographically remote from the organisation's central management because the local business operation may not be subject to adequate corporate level scrutiny, and local management does not recognise the need for fraud and corruption control measures.

CIT must communicate to all line personnel of discrete business units, particularly business units that are geographically remote to CIT's core business functions, that they are accountable for fraud and corruption control within their business unit.

Awareness raising of fraud and corruption risk

CIT must implement a program aimed at ensuring that the governing body (the CIT Board), top management, specialist fraud and corruption resources, line engagement, students and all other personnel, are aware of CIT's fraud and corruption exposures and how they must respond if they detect or suspect a fraud or corruption event.

Overall responsibility for ensuring that this program is implemented rests with the governing body and top management, with day-to-day aspects being delegated to the specialist fraud and corruption control function.

Matters to be covered in a fraud and corruption awareness-raising program

A fraud and corruption awareness training program must be delivered regularly, appropriate to CIT's exposure to fraud and corruption risk, and so that it is relevant and useful to the position and role of each person in CIT.

Such a program must include the following elements:

- a clear statement of CIT's definitions of behaviours that constitute fraud or corruption

- an unequivocal statement that fraudulent and corrupt practices within CIT will not be tolerated

- the incidence of fraud and corruption

Note – in the current age this should include a consideration of fraud and corruption trends globally particularly as CIT sometimes operates outside of Australia.

- fraud and corruption exposures in the industry sectors and jurisdictions in which CIT operates

- the types of fraud and corruption that have been detected at CIT in the previous five years, and how those matters were dealt with in terms of disciplinary action and internal control enhancements

- a clear statement about what is expected of management and staff if fraud or corruption is detected or suspected

- a statement as to how management and staff and students can report allegations or concerns regarding fraud or unethical conduct including CIT's policy for the protection of whistle blowers

- an overview of CIT's FCCF

- an overview of resources allocated to fraud and corruption control

- an overview of fraud and corruption red flag behaviours.

Additionally, fraud and corruption awareness and standards of conduct should be promoted through regular meetings within each CIT business unit, staff and student newsletters and other internal methods of communication.

Fraud and corruption risk management

Fraud and corruption are business risks and will have a similar impact on CIT as other types of enterprise risk including:

- financial loss

- loss of information

- penalties imposed on CIT by courts and regulators

- reputational impact

- diversion of management energy

- organisational morale

- 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.
- Note: other risk management approaches can also be used e.g., three lines of defence.

External environment scan

CIT will systematically scan and monitor the external environment to identify fraud and corruption risks to which CIT may be exposed. These risks may be in the nature of threats facing CIT and 'fraud and corruption drivers' in the industries and jurisdictions in which CIT operates. External environment scanning should include identifying and analysing relevant events, trends and drivers, by searching the elements outlined in the table below.

‘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
- presentations.

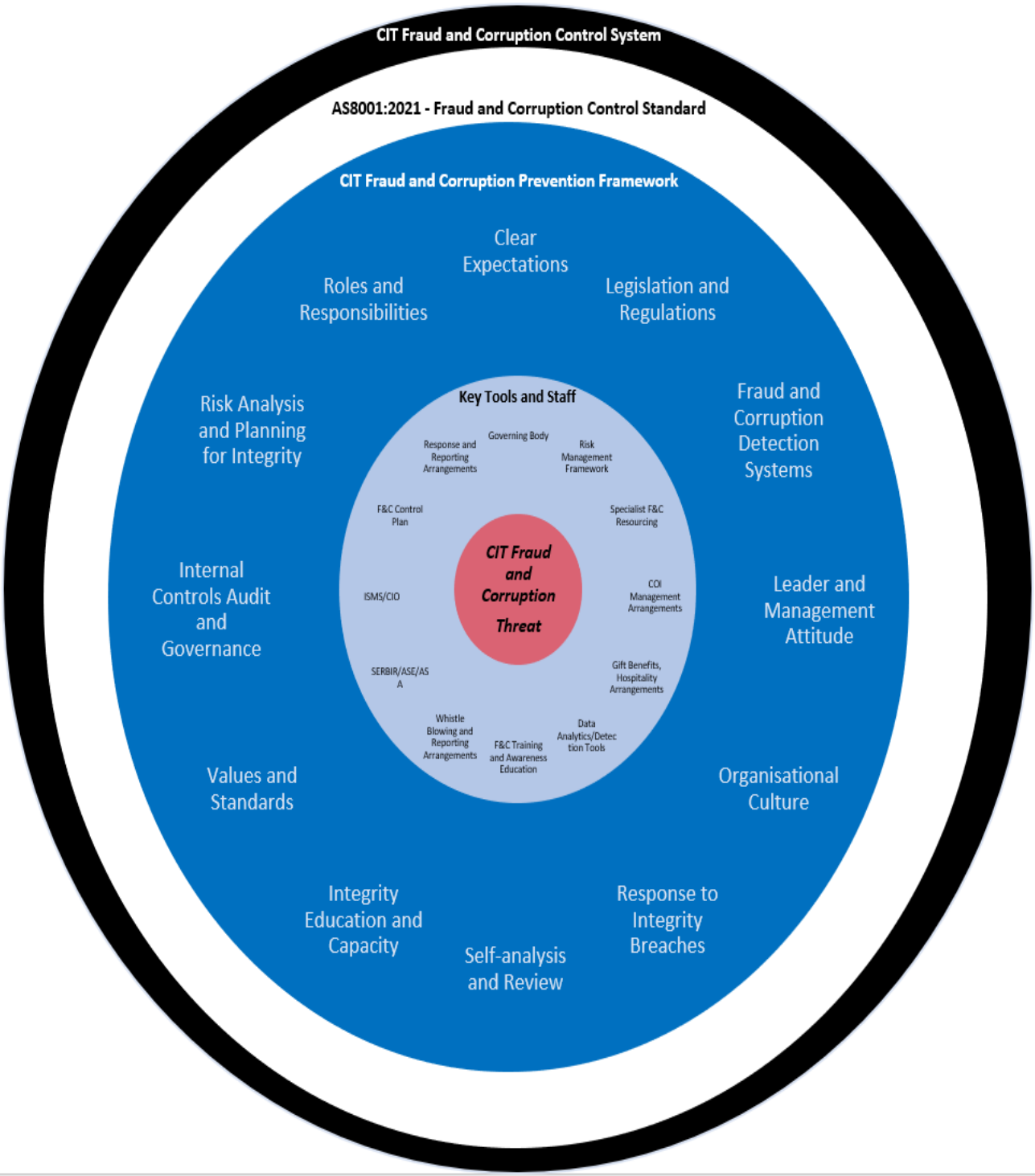
In accordance with the CIT Risk Management Context, the PESTLE scan, and risks identified as part of that scan, will link with the CIT Strategic Risk Register. Under this model, CIT identifies a strategic fraud and corruption risk. The PESTLE scan provides detailed analysis of the specific risks which may occur.

Developing and implementing a fraud and corruption control system

General

CIT will develop and implement a FCCF, incorporating CIT's approach to controlling fraud and corruption exposures at strategic and tactical operational levels.

CIT Fraud and Corruption Control



In preparing and implementing such a system, CIT will analyse the following:

- contextual factors including CIT's size, composition, head count, geographic footprint and risk profile
- industries in which CIT operates
- economies, markets and jurisdictions in which CIT operates with particular regard to applicable laws and regulations.

The FCCF will seek to control:

- internal fraud and corruption against CIT and its operations
- external fraud and corruption against CIT and its operations
    - fraud and corruption involving persons internal to CIT in collaboration with persons external to CIT
    - fraud and corruption by CIT or by persons purporting to act on behalf of and in the interests of CIT.

The FCCF will include CIT's intended action in implementing and monitoring CIT's fraud and corruption prevention, detection and response initiatives.

It is important that CIT views the FCCF as an integral part of an overall risk management system, on the premise that fraud and corruption are business risks that are controllable by the application of risk management principles.

Ultimate accountability for the implementation, and ongoing monitoring and maintenance of the FCCF, rests with the governing body (CIT Board) and is achieved via the CIT fraud and corruption control function.

The FCCF will consider any existing policies and procedures relevant to fraud and corruption risk, including:

- ACTPS Code of Conduct
- ACT Public Service Integrity Governance Policy (2022).

The FCCF should be viewed as a comprehensive framework for addressing fraud and corruption risk with appropriate linkages to other CIT wide pronouncements aimed at reducing CIT's fraud and corruption exposures.

In developing the FCCF, interested internal and external parties – and, where appropriate, regulators – should be consulted as broadly as possible. The FCCF should have a foundation of broad-based consultation and support to ensure it is effective.

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. Roles and responsibilities

The table below describes the roles and responsibilities of CIT staff in the FCCF.

Element Custodian Responsibility Status	Element Custodian Responsibility Status	Element Custodian Responsibility Status
Clear expectations	CEO	Accountable for developing, implementing and reinforcing expectations, and acting on non-compliance.
	SERBIR / ED Corporate / EBM Governance	Primary responsibility for implementation of the CIT Integrity Framework, with some associated functions outlined in the Financial Instructions. SERBIRs are appointed to manage the integrity requirements under the *PSM Standards 2006* (part 2.3), which includes implementing integrity strategies and processes to detect and investigate fraud and corruption. In addition, the SERBIR deals with: • risk management for integrity and fraud and corruption prevention planning • reporting of fraud and corruption • referral of corruption allegations and public interest disclosures.
	SERBIR and all Executive Directors	Responsible for implementing, reinforcing and advising on expectations.
	EBM Audit, Risk and Corporate Governance	Responsible for ensuring expectations are professionally written, accessible (on intranet) and maintained/current.
	Individuals	Responsible for complying with expectations and holding each other to account.
	ACT Integrity Commission	Responsible for: • investigating conduct that is alleged to be corrupt • referring suspected instances of criminality or wrongdoing to the appropriate authority for further investigation and action • preventing corruption, including by researching corrupt practices and mitigating the risks of corruption • publishing information about investigations conducted by the commission, including lessons learned • providing education programs about the operation of the *Integrity Commission Act 2018* and the commission, including providing advice, training, and education services.

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 management. Results of these reviews will be directly reported to the CEO. The Audit and Risk Committee must also establish a Charter to outline the key objectives and function of the Committee.
Fraud and corruption detection systems	CIT Board, SERBIR, all Executive Directors, Audit and Risk Committee, EBM Audit, Risk and Corporate Governance and risk owners	See Section 7 - Fraud and corruption detection systems.

Element Custodian Responsibility Status	Element Custodian Responsibility Status	Element Custodian Responsibility Status
Values and standards	CIT Board, SERBIR, all Executive Directors, Audit and Risk Committee, EBM Audit, Risk and Corporate Governance, risk owners and human resources.	Responsible for demonstrating by example, appropriate behaviours and acting on integrity issues.
Leadership and management attitude	CIT Board, SERBIR, all Executive Directors, Audit and Risk Committee EBM Audit, Risk and Corporate Governance, risk owners and human resources.	Responsible for demonstrating by example, appropriate behaviours and acting on integrity issues.
Organisation culture	CIT Board, SERBIR, all Executive Directors, Audit and Risk Committee, EBM Audit, Risk and Corporate Governance and human resources.	Responsible for demonstrating by example, appropriate behaviours and acting on integrity issues
Integrity education and capacity	CIT Board, SERBIR, all Executive Directors, Audit and Risk Committee, EBM Audit, Risk and Corporate Governance, risk owners and human resources.	Responsible for the analysis, design, development, implementation and evaluation of CIT integrity training (including the provision of adequate resources and systems to do so)
Response to integrity breaches	CEO, Board, SERBIR, all Executive Directors, Audit and Risk Committee, EBM Audit, Risk and Corporate Governance, risk owners and human resources.	See section 11 – Be Accountable for Integrity
Self-analysis and review	CEO, CIT Board, SERBIR, all Executive Directors, Audit and Risk Committee EBM Audit, Risk and Corporate Governance, risk owners	See section 12 – Self-analysis and review

Element Custodian Responsibility Status	Element Custodian Responsibility Status	Element Custodian Responsibility Status
Oversight	CEO, Board, SERBIR, all Executive Directors, Audit and Risk Committee, EBM Audit, Risk and Corporate Governance and risk owners.	See section 13 –Oversight
Authority head	CEO	Accountable for integrity overall · Set expectations · Oversight of framework
Integrity committee	EBM HRW / SERBIR	Identify, share and support good integrity practice across functional areas. Promote awareness of fraud and corruption risks, and strategies to detect events outside of standard, normal or expected practice. Routinely report on its work and integrity related trends to senior leadership team Recommend new actions or initiatives to support integrity
Directors and managers	Senior Directors, Directors, Senior Managers and Managers	Promote integrity and prevent misconduct and corruption Ensure internal controls, policies and procedures are operationalised Ensure obligations are met Model appropriate behaviours and standards Manage, respond to and report integrity breaches or issues as they arise

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
Public Sector Management Act 1994 (ACT) (PSM Act)	Part 2 of the PSM Act establishes the legal and ethical framework for the ACTPS. Employees should be mindful of their obligations under Division 2.1 of the PSM Act which sets out the values and general principles that public servants must adhere to in their day-to-day work. Section 7 of the PSM Act identifies the meaning of the Public Sector Values and how they are to be used and applied in an employee's work. Section 9 of the PSM Act articulates the expected conduct and behaviour of all employees. This includes but is not limited to; an employee must take all reasonable steps to avoid a conflict of interest and an employee must not behave in a way that is inconsistent with the public sector values or undermines the integrity and reputation of the service. It is also expected that an employee must not take improper advantage of their position or information gained through their position or improperly use an Australian Capital Territory ('Territory') resource, including information, accessed through their job. Part 2.3 of the repealed Public Sector Management Standards 2006 (PSM Standards 2006) refers to Fraud and Corruption responsibilities for Director Generals. Section 113 of the Public Sector Management Standards 2016 (PSM Standards 2016) states that Part 2.3 (PSM Standards 2006) continues to apply, despite the repealed standard. DGs and CEOs must ensure that risks to integrity of the directorate/agency are: (a) assessed and treated in accordance with the Risk Management Standard and the associated policy guidance; and (b) addressed in detailed fraud and corruption prevention plans.
Integrity Commission Act 2018	Under s 57 - Any person may make a complaint to the commission about conduct that may be corrupt conduct (a corruption complaint). Under s 62(1) - The following people must notify the commission about any matter the person suspects on reasonable grounds involves serious corrupt conduct or systemic corrupt conduct: (a) the head of a public sector entity; (i.e., CIT CEO) (b) an SES member (i.e., CIT Executives)

Legislation, standards, Policy or Framework	Description of obligation
Public Interest Disclosure Act 2012	Under s14 - Any person may disclose disclosable conduct 3. Under s17 (2) Disclosure officer must give copies of disclosures of disclosable conduct to the Integrity Commissioner. Under s11(2) of the PID Act requires that public sector entities: • nominate at least one person to be a disclosure officer for disclosures of disclosable conduct; • publish the contact details for all nominated disclosure officers on the public sector entity's website; and • give the contact details of all disclosure officers to the Commission.
ACT Public Service Integrity Governance Policy (2022)	All CIT employees must promote integrity and prevent misconduct, including fraud and corruption. The Integrity Governance policy applies to all ACT Government directorates and public sector bodies (including CIT) in relation to public employees and executives employed in the ACTPS under the Public Sector Management Act 1994 (ACT) (PSM Act). Integrity also applies to CIT board, committee members, contractors and consultants. In the Integrity Governance Policy, these people are referred to as employees and include an officer, temporary employee, casual employee, public sector member and a member of the senior executive service. The CIT CEO must ensure that risks to integrity of CIT are assessed and treated in accordance with the Risk Management Standard and the associated policy guidance and addressed in detailed fraud and corruption prevention plans. The CIT CEO must ensure that the integrity arrangements within the directorate/agency are assessed and reviewed every 2 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 The CIT CEO must establish and maintain an information system that records- all: instances of fraud and corruption; referrals to the Integrity Commission; losses to the directorate/agency or potential for damage to the reputation of the directorate/agency or ACTPS; investigative action taken; (e) disciplinary action taken or outcomes of matters which have been prosecuted; and

[3] Disclosable conduct means an action or a policy, practice or procedure of a public sector entity, or public official for a public sector entity, that— (a) is maladministration; or (b) results in a substantial and specific danger to public health or safety, or the environment.
Disclosable conduct does not include an action or a policy practice or procedure of a public sector entity, or a public official for a public sector entity, that— (a) relates to a personal work-related grievance of the person disclosing the conduct; or (b) is to give effect to a policy of the Territory about amounts, purposes or priorities of public expenditure.

	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. The CIT CEO must include details of the implementation of the fraud and corruption prevention plans in the Annual Report to the Minister.
Public Sector Management Standards 2006	(Repealed, Part 2.3 remains active) Under Part 2.3 of the Public Sector Management Standards 2006, CIT is required to develop and implement a CIT Fraud and Corruption Prevention Plan.
ACTPS Integrity Framework (2022)	The Integrity Framework applies to all ACT Government directorates and public sector bodies in relation to public employees and executives employed in the ACTPS under the Public Sector Management Act 1994 (PSM Act) including CIT. Integrity also applies to CIT board and committee members and contractors or consultants. The CIT CEO has a responsibility to ensure that all employees within their directorate or agency are aware of the Integrity Framework. It is important that CEOs model, support and promote a culture of integrity which will assist in instilling high trust and performance.
ACTPS Integrity Governance Policy (2022)	CIT is required to appoint an individual as the Senior Executive Responsible for Business Integrity Risk (SERBIR). The SERBIR has primary responsibility for the implementation of the Integrity Framework with some associated functions outlined in the Financial Instructions. SERBIRs are appointed to manage the integrity requirements under the PSM Standards 2006 (part 2.3) which includes implementing integrity strategies and processes to detect and investigate fraud and corruption. The CIT CEO must ensure that risks to integrity of CIT are: (a) assessed and treated in accordance with the Risk Management Standard and the associated policy guidance; and (b) addressed in detailed fraud and corruption prevention plans.
Director General Instructions	The CEO / Director – General has delegated Authority under the FMA s54 for the efficient and effective financial management of their respective organisation's resources. This delegation can be sub-delegated to Executives/ Senior staff in the organisation. (See the Financial Delegations Better Practice Guide 2007) These Instructions are designed to provide clear direction about key compliance obligations with respect to resource management. Its underlying premise is the prevention of Fraud and Corruption and the promotion of Integrity. The Financial Delegations assigned to directorate positions are listed in the organisation's own CEFI document.
Financial Management Act 1996	Sets out directorate requirements for Budgets, Financial Reporting, Borrowings and Governance. Responsibility is

	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.

	Those with responsibilities under the PID Act (such as the Commission, CIT and disclosure officers) must not use or share 'protected information' recklessly.
CIT Fraud and Corruption Prevention Plan	Under Part 2.3 of the PSM Standards 2006, directorates/agencies are required to develop and implement a Fraud and Corruption Prevention Plan. The preparation of this plan follows on from the formal risk assessment of the directorate/agency.

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 other risks that may have a material consequence yet lower rating. It is important for management to continue to monitor all risks identified as being moderate or higher and to ensure a treatment plan exists for each of these risks.

The CIT fraud and corruption risk assessment will be formally updated at least every two years and part of the Fraud and Corruption Control Plan. The CIT Corporate Services Executive Director is responsible for this update which will include: updating the assessment of existing risks for changes in treatments, consequences or likelihood ratings if changes are deemed necessary:

- removing risks which are no longer relevant
- identifying any new risks which should be included and addressed as part of the ongoing risk management process
- updating the action plans to address the risks for new key risks
- identifying new treatment strategies/action plans

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.

CIT will include references to behavioural values and standards in all job advertisements, staff performance processes and on the CIT website (including the pathways available to report non-compliance with the code of conduct).

Leadership and management attitude

CIT will ensure all recruitment practices encompass strategies to attract, select and recruit new and future leaders who possess and demonstrate integrity.

CIT will develop and provide executive level programs and activities to develop the skills and knowledge of leaders with respect to integrity (including skills and knowledge to manage integrity in and across their teams).

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).

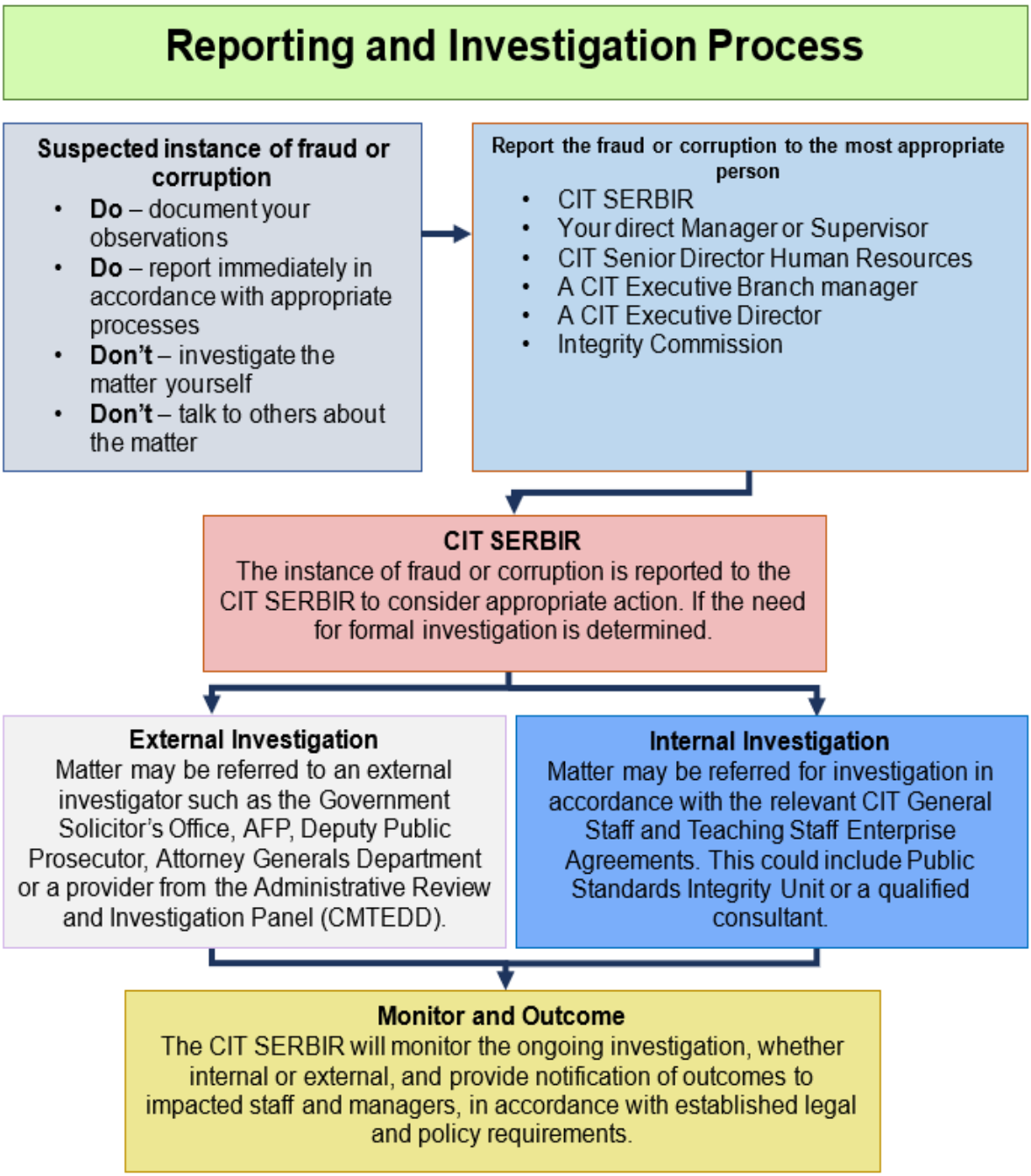
Refer also to Reporting and Investigation Process enclosed further below

ACT Reportable Conduct for the ACT Community (including students)

Members of the community and/or CIT students who have information about reportable conduct should advise CIT using CIT's complaint process. Members of the community and/or CIT students may also need to report significant harm or abuse to other agencies, for example ACT Policing or Child and Youth Protection Services. If criminal conduct is suspected to have occurred, members of the community and/or CIT students should first report to the police.

Reporting and Investigation Process

CIT responds to and investigates fraud and corruption activities via the process described in the table below.



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. OBJ

13. Oversight

The oversight of fraud and corruption activities and integrity aspects more broadly is detailed in Section 4 - Roles and Responsibilities. In practice, these fraud and corruption risks and activities are to be reported as standing agenda items at the CIT Board meetings, Audit and Risk Committee meetings and Executive Management Committee meetings as standing agenda items.