FRAUD AND CORRUPTION CONTROL PLAN

Date: March 2023

Review: November 2024

Contents

1. INTRODUCTION

The Fraud and Corruption Control Plan (FCCP) documents the strategic and operational approach to mitigating fraud and corruption within South West TAFE (the organisation). It provides an overview of how fraud and corruption risks will be managed and complies with the Australian Standard AS ISO 31000:2018 Risk Management: Guidelines.

The organisation is committed to preventing and controlling fraud and corruption whether initiated within the organisation or externally.

2. PURPOSE

This plan aims to further:

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

3. DEFINITIONS

3.1. Fraud

In accordance with the FCCP, fraud against the organisation is defined as:

'Dishonest activity causing actual or potential financial loss'

Examples of the types of conduct that would fall within the organisation's definition of fraud include (but are not limited to):

- theft
- accounting fraud (false invoices, misappropriation etc.)
- unlawful use of, or obtaining property, equipment, material or services
- causing a loss, or avoiding and/or creating a liability
- providing false or misleading information to the Institute, or failing to provide it when there is an obligation to do so
- misuse of organisation assets, equipment or facilities
- making, or using false, forged or falsified documents, and
- wrongfully using organisation information or intellectual property.

3.2. Corruption

AS/NZ 8001:2008 – Fraud and Corruption Control, defines corruption as:

"Dishonest activity in which a director, executive , manager, employee or contractor of an entity acts contrary to the interest of the entity and abuses his/ her position of trust in order to achieve some personal gain or advantage for him or herself for another person or entity".

4. INTERNAL CONTROL SYSTEM

The organisation has a strong system of internal controls, including our governance, risk management and policy frameworks.

These controls are operationalised by a range of security and audit functions across the organisation by the departments; ensuring that fraud and corruption risks are considered in business as usual activities.

Ultimate responsibility remains with the Board. The Audit, Risk and Compliance Committee is responsible for the oversight of the organisation's fraud and corruption control arrangements and ensures that the organisation has appropriate processes and systems in place to detect, capture and effectively respond to fraud and corruption.

The CEO is committed to the active prevention of corrupt or fraudulent activities in a systematic way in order to enhance the operation and reputation of the organisation.

---

5. FRAUD & CORRUPTION CONTROL FRAMEWORK

Fraud control is further ensured not only by the implementation of Australian Government legislative requirements but by the adoption and promotion of practices recommended by the Australian National Audit Office (ANAO) and other organisations (e.g. Better Practice Guides). The organisation has adopted the key elements of Fraud Control Framework recommended in the *ANAO Better Practice Guide: Fraud Control in Australian Government Entities 2011*.

The Fraud Control Framework provides an overarching approach to effective fraud control within the organisation. The Executive and Senior Management set the 'tone at the top' by creating an ethical culture where staff are encouraged to identify and manage potential fraud risks.

Adapted for this publication from ANAO Fraud Control in Australian Government Entities 2011

5.1. Leadership & Culture

Setting the right 'Tone at the top' is critical to fraud control within the organisation. The Board and Executive Team are committed to providing a strong organisational culture based on sound ethics and integrity to ensure effective fraud control.

5.2. Policy, Legislation & Governance

The organisation has a strong alignment to policy and legislation to ensure all mandatory requirements are met. The organisation's governance structure identifies the level of accountability and responsibility for the Board, CEO and Executive team in relation to risk and fraud alignment.

5.3. Fraud Control Strategies

Key fraud control strategies contributing to effective fraud control consist of prevention, detection, response and monitoring, evaluating and reporting. The organisation through the FCCP ensures that these strategies are embedded within the organisation to assist with the prevention of fraud and corruption.

---

6. ROLES, RESPONSIBILITIES, ACCOUNTABILITIES

Board

The Board hold the overarching responsibility for monitoring the control and prevention of fraud, corruption and other losses.

Audit, Risk & Compliance Committee

The Audit, Risk and Compliance Committee support the Board in meeting its responsibilities of monitoring the control and prevention of fraud, corruption and other losses and shall report to the Board where applicable.

Executive and Management

The CEO, Executive Managers and Senior Managers of the organisation must be committed to the active prevention of corrupt or fraudulent activities in a systematic way in order to enhance the operation and reputation of the Institute.

All senior managers must ensure there are mechanisms in place within their area of control to:

- identify and assess the risk of corruption, theft and fraud
- encourage a culture of honest and ethical behaviour, and
- educate employees about corruption and fraud prevention and detection.

The CEO and CFO are expected to bring to the notice of the Audit, Risk & Compliance Committee any potential areas of fraud and corrupt activities as required, and enforce and develop procedures to control and monitor these areas.
An annual fraud activities report will be provided to the Audit, Risk & Compliance Committee.

Audit, Risk & Compliance Department

The Audit, Risk & Compliance (ARC) Department in conjunction with the CFO will coordinate the implementation and monitoring of the Fraud & Corruption Control Plan, including all related policies and guidelines. The ARC Department holds primary responsibility for the coordination of the Speak Up Service and ensuring all reports through this service are assessed and where appropriate investigated.

Public Interest Disclosure Co-ordinator

All correspondence, phone calls and emails from internal or external protected disclosures will be referred to the Public Interest Disclosure Co-ordinator.

All Staff

All SWTAFE staff have the responsibility to report suspected corrupt, theft and/or fraudulent activity. Any staff member who suspects such activity should take all reasonable steps to make the organisation aware of such an activity in line with the organisation's reporting mechanisms discussed below.

Students
Students are encouraged to report suspected corrupt, theft and/or fraudulent activity to their teacher, senior educator or Student Services.

---

7. ETHICAL CULTURE

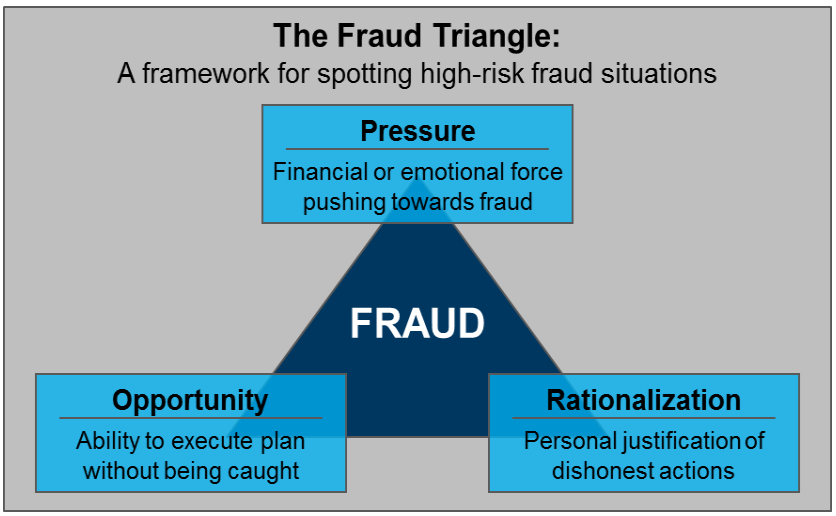
7.1. Understanding why people commit fraud – The Fraud Triangle

The Fraud Triangle describes the three key contributing elements to fraud within the organisation. These three elements are:

1. Pressure
2. Opportunity
3. Rationalisation

Raising awareness of the above three contributing elements can support an ethical culture and assist staff in recognising early warning signs of fraudulent activity.

Figure 1 – The Fraud Triangle



Brumell Group: The Fraud Triangle Theory

7.2. Embedding an ethical culture

The Fraud and Corruption Control Policy and Guideline establish a fundamental strategy in controlling the risk of fraud and corruption in the development and maintenance of a sound ethical culture across the organisation. Raising awareness of ethical behaviours will assist in minimising the risk of fraud across the organisation.

The organisation's expectations on ethical behaviour are outlined in the Code of Conduct which describes its commitment to creating and maintaining standards of behaviour and principles of good conduct aligned to the organisation's stated values.

8. FRAUD PREVENTION

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

The organisation has implemented a number of prevention strategies which are outlined below.

8.1. Fraud Awareness Training

The People & Culture Department's recruitment process requires all new staff to read and acknowledge the requirements of key organisation policies. Fraud awareness training has been incorporated into SWTAFE's On-boarding process which all new employees must complete upon commencement with the organisation.

The organisation has also developed a suite of training modules for all staff to complete on an annual basis which includes fraud and corruption.

8.2. Fraud Risk Management

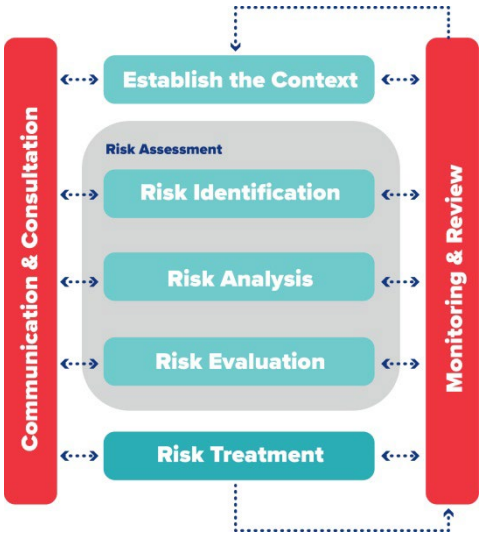
Fraud Risk management is an integrated part of the organisation's overall Risk Management Framework. Fraud risk assessments are conducted 'face-to-face' with each department periodically by the relevant manager. This enables the departments to raise any concerns directly with the manager to ensure clarity and accuracy in compiling the assessment.

To maximise the effectiveness of the fraud risk assessment process, the assessments will:

- be comprehensive, covering as far as possible, all potential fraud risks in all divisions at all locations
- aligning to the organisation's adopted risk assessment process
- separately consider inherent risk and internal control

Risk Assessment Process

The organisation's Risk Assessment process has been adopted in accordance with the AS ISO 31000:2018 Risk Management: Guidelines standards.



The risk assessment process consists of the following elements:

- **Communication & Consultation -** Communication and consultation with external and internal stakeholders should take place during all stages of the risk management process to understand the interests of stakeholders, ensure risks are adequately identified and secure endorsement for actions to address risks.
- **Scope, context and criteria –** establishing the scope, context and criteria is to customise the risk management process, enabling effective risk assessment and appropriate risk treatment. Scope, context and criteria involve defining the scope of the process, and understanding the external and internal context.
- **Risk identification -** The risk identification approach is used to find, recognise and describe any events that, if they were to occur could have a negative impact on the organisation.
- **Risk Analysis -**Risk analysis determines the risk level against the risk criteria by understanding how quickly the risk can occur, the sources and cause of a risk, the consequences and likelihood of those consequences. Analysis takes into account the effectiveness of existing controls.
- **Risk Evaluation** - Risk evaluation involves comparing the results of the risk analysis with the established risk criteria to determine where additional action is required. This approach is conducted by the organisation through a risk assessment process of applying a consequence and likelihood matrix.

  Please refer to Appendix 3.1 to review the risk matrix
- **Risk Treatment -** Risk treatment includes selecting appropriate controls for modifying risks and implementing these options.
- **Monitor & Review -**The organisation's environment is constantly changing and hence the organisation needs to continually monitor and review its risks and the effectiveness of its risk management process (including controls and treatment plans).

Risk Management Framework

The organisation's Risk Management Framework consists of a set of components that support and sustain risk management throughout the organisation. The key elements of the framework are outlined below and are essential for a strong risk management framework.

Figure 1: Risk Management Framework Elements

The Risk Management Framework Elements:

Leadership& Commitment: Commitment from the organisation's Board and Executive Team to identify the management of risk as an integral part of its operations, focusing on strategies to minimise risks to the organisation's ambition, purpose and values.

Integration: Integrating risk management into every part of the organisation's structure, with all employees having responsibility for managing risk.

Design: establishment of the risk management framework including the policy, accountability and reporting mechanisms.

Implementation: implementation of the framework and the embedding of the risk management process within the organisation.

Evaluation: monitor and reviewing of the framework to assess the effectiveness of its design and implementation.

Improvement: continuous improvement should be identified and implemented.

8.3. Recruitment & Pre-employment Screening

The organisation conducts recruitment & pre-employment screening for all new employees in line with the recruitment and selection guidelines. Screening requirements under the recruitment and selection guidelines include:

- Police Check
- Working With Children Check
- Evidenced Reference Checks
- Verification of formal qualifications

8.4. Annual Leave Monitoring and Requirements

The organisation's Leave Arrangements Policy and Procedure identifies the maximum annual leave provisions and the requirements of management to ensure all employees do not exceed this limit.

Where employees are in excess of the maximum annual leave provisions an annual leave plan will be developed to reduce the excess entitlements within a three month period.

Please refer to the Leave Arrangements Policy and Procedure for further details.

8.5. Contract Management

The organisation has embedded strong contract management processes to reduce the risk of fraud and corruption with our external engagements. A number of processes have been put in place to ensure appropriate due diligence has occurred with all contracts across the organisation, including training and business contracts along with contractor and supplier engagements.

Contractor and Supplier Due Diligence

The organisation will perform effective due diligence on contractors and suppliers with the following mandatory requirements to be completed prior to engagement:

- Relevant qualifications and appropriate licences
- Current national Police History Check (NPHC)
- Working With Children Check (WWCC), where applicable
- Insurance checks
- Confidentiality Agreement
- ABN Confirmation

Further requirements may be completed where applicable.

8.6. Student Qualification Verification

The organisation has "authentication" processes that must be followed prior to granting a student with credit or acknowledgement of previously achieved Competencies. This process is documented in the Institute's "Authenticating a Statement of Attainment" Business Process.

8.7. Declaration of Interest and Conflict of Interest

The organisation ensures that its employees and directors understand the detrimental impact to the organisation of conflicts of interest and have incorporated this into the Institute's workplace inductions. The Declaration of Interest Policy along with the Gifts, Benefits & Hospitality Policy and Guidelines provide guidance to staff and directors on what to do if a conflict of interest has been identified.

Along with this it is a mandatory requirements that all Board Directors and the Executive Team complete a declaration of private interest upon appointment and annually thereafter.

8.8. Records Management

Records management is an integral part of SWTAFE's operations to ensure it can meet its regulatory and legislative obligations. The organisation must be records management compliant with various legislations and standards and as such strong processes are required to ensure records are managed and retained appropriately and in line with these requirements.

8.9. Policies, Procedures and Guidelines

The organisation has a number of policies, procedures and guidelines that assist in preventing fraud across the organisation. Some of these consist of:

- Code of Conduct
- Fraud, Corruption and Other Losses Policy
- Financial Delegations Policy
- Issue and use of Credit Card Policy
- Procurement Policy & Guidelines
- Use of ICT Facilities and Services Guidelines
- Gifts, Benefits and Hospitality Guidelines
- Declaration of Interest Policy
- Related Party Disclosure Policy
- Related Party Disclosure Guidelines
- Recruitment and Selection Guidelines
- Leave Arrangements Policy
- Risk Management Policy
- Money Collection & Handling Procedure
- Plagiarism Guidelines
- Copyright Guidelines

---

9. FRAUD DETECTION

The organisation understands that despite the prevention strategies put in place, fraud and corruption may still occur. Therefore it is important to have strategies in place to detect fraud as soon as possible if it has occurred.

The organisation has implemented a number of detection strategies which are outlined below.

9.1. Fraud Reporting Mechanisms

Internal and external fraud reporting mechanisms are available on the organisation's intranet and internet. Guidance on how to report suspected fraud or corruption is provided in the Fraud, Corruption and Other Losses Guidelines. The guidelines provide the internal and external reporting lines and also provide an overview of the reporting and investigation process. The reporting mechanisms ensure the confidentiality of the information received from anyone wishing to report a suspected case of fraud.

Speak Up Service
Speak Up is an independent service that allows SWTAFE employees to raise concerns of suspected fraud, corruption and serious misconduct without fear of retribution or reprisal.

It is designed to support staff to feel safe to report suspected fraud, corruption and serious misconduct (e.g. serious conflicts of interest). Speak Up is not designed for all workplace matters and does not replace existing ways to raise concerns or make complaints. It is encouraged that all issues are raised with your relevant manager in the first instance; this is the best way to reach a quick solution.

Speak Up contributes to the organisation's efforts to support a confident reporting culture where we all feel safe to question inappropriate behaviour.

9.2. Public Interest Disclosure

The *Public Interest Disclosure Act 2012* (Vic) enables people to make disclosures about improper conduct within the public sector without fear of reprisal. The Act aims to ensure openness, transparency and accountability by encouraging people to make disclosures and protecting them if, and when, they do so.

The organisation is committed to the aims and objectives of the *Public Interest Disclosure Act 2012* and encourages the disclosure of improper conduct relating to the Institute, or a Board member, officer, or employee of the organisation, in accordance with the Act.

The organisation does not tolerate improper conduct by the organisation, its Board members, officers and employees nor does it tolerate reprisal against any person who discloses such conduct.

Information about the Public Interest Disclosure Act is available for all staff on the intranet and also forms part of the annual training framework to ensure staff have an understanding of the aims and objectives of the act.

9.3. Internal Audit

Internal Audit is an independent function within the organisation that reports directly to the Audit, Risk and Compliance Committee. They conduct better practice assurance activities, audits and assurance advisory services which assist in the development of efficient and effective systems of internal control, risk management and corporate governance.

The annual audit plan is developed through a review of the organisations Risk Register and Strategic Plan.

9.4. External Audit

The organisation's financial statements are audited by the Victorian Auditor General Officer appointed auditors and as such are familiar with the role and responsibilities of the auditor in detecting fraud.

The Executive Team and the Audit, Risk and Compliance Committee will undertake a discussion with the auditor in terms of the audit procedures that will be carried out during the audit that are aimed at detecting material misstatements in the organisation's financial statements due to fraud or error.

9.5. Data Analysis

Data Analysis is an effective way of identifying fraudulent or corrupt activity within the organisation through post-transactional reviews, data mining and analysis of management accounting report. Such strategies not only assist with the detection of fraudulent activity but also assist in preventing fraudulent activity as the threat of detection may be enough to deter a staff member who would otherwise be motivated to engage in fraud and corruption.

---

10. FRAUD RESPONSE

In accordance with the AS ISO 31000:2018 Risk Management: Guidelines standards the organisation ensures that response strategies are in place to address fraud and corruption activity.
The organisation has implemented a number of response strategies as outlined below.

10.1. Investigation

Internal Investigation

To ensure that allegations of fraud and corruption are investigated appropriately, the organisation will conduct investigations in accordance with the Fraud and Corruption Control Guidelines. Upon receipt of preliminary findings of the initial investigation conducted by the organisation, the matter may be escalated to the relevant external authority for further investigation.

External Investigation

An investigation into apparent or suspected fraud and corruption should be conducted by appropriately skilled and experienced personnel who are independent of the organisation, these independent agencies include:

- Independent broad-based anti-corruption commission (IBAC)
- Victorian Ombudsman
- Victoria Police
- The CEO of South West TAFE has an obligation to notify IBAC of any suspected matter which they suspect on reasonable grounds that corrupt conduct has occurred or is occurring.

10.2. Reporting Processes

The organisation has zero tolerance for fraud and corruption and will report any instances of alleged fraud or corruption in accordance with mandatory compliance requirements.

Standing Directions of the Minister for Finance 2018

The organisation reports actual or suspected fraud, corruption and other losses in accordance with the Direction 3.5.3 of the Standing Directions of the Minister for Finance 2018.

Direction 3.5.3:

Where an Agency is made aware of an actual or suspected Significant or Systemic Fraud, Corruption or Other Loss, the Accountable Officer must:

(a) notify, as soon as is practicable, the Responsible Minister, Audit Committee, Portfolio Department and Auditor-General of the incident and remedial action to be taken;

(b) ensure that the persons notified under Direction 3.5.3(a) are kept informed about the incident, including the outcome of investigations; and

(c) ensure that the Agency takes appropriate action to mitigate against future Fraud, Corruption and Other Losses.

Instances involving the following will be required to be reported in accordance with Direction 3.5.3:

- values **greater than $5 000 in cash**
- values **greater than $50 000 in property**
- values **greater than $1000 for purchasing and prepaid debit cards**

The provided template will be utilised in the reporting of significant or systemic Fraud, Corruption and Other Losses.

Notifiable Data Breach – Privacy Act 1988

The Notifiable Data Breaches (NBD) scheme under Part IIIC of the Privacy Act 1988 establishes the requirements for entities in responding to data breaches. Where any Information Security breach has been confirmed or is suspected, SWTAFE is required to report the breach in line with the relevant policy and scheme.

Under the Notifiable Data Breach (NDB) scheme, SWTAFE is obliged to:

> *"to notify individuals whose personal information is involved in a data breach that is likely to result in serious harm. This notification must include recommendations about the steps individuals should take in*

response to the breach. The Australian Information Commissioner (Commissioner) must also be notified of eligible data breaches."

Where a breach has been identified, the Manager, ICT and Innovation (or equivalent) must be alerted to investigate any potential breach and reporting undertaken via www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme

Reporting Fraud
Where it is necessary for the organisation to report suspected fraud or corruption to a law enforcement agency the following items will be provided:

- a summary of the allegations.
- a list of witnesses and potential witnesses.
- a list of suspects and potential suspects.
- copies of all statements, depositions or affidavits obtained to that point including and in particular, any written statement made by the subject of the investigation.
- a copy of the transcript of any interview conducted with a person suspected of involvement in the matters alleged.
- a copy of any electronic media on which such interviews have been recorded. Copies of all documentary evidence obtained to that point (ultimately the law enforcement agency will probably require the original documents, in which case copies should be retained by the Council).
- any charts or diagrammatical summaries of the allegations and evidence that the Council may have produced.

Fraud and Corruption Incident Register
A fraud and corruption incident register is maintained through the CEO's Office with all incidents of fraud and corruption held within. The organisation reviews the register on an annual basis as part of a continuous improvement strategy and to assist in identifying trends within the organisation.

10.3. Disciplinary Procedures
To ensure substantiated incidents of fraud or corruption are dealt with appropriately, the organisation will follow the processes governing the reporting of improper conduct within the organisation and take appropriate remedial action under the Code of Conduct and Unacceptable Behaviour Policy.

10.4. Recovery of Stolen Funds or Property
SWTAFE will actively pursue the recovery of any money or property lost through fraud, and where appropriate seek criminal or civil action. The recovery of losses will help to limit any reputational damage SWTAFE may suffer and the financial impact this may have on SWTAFE's objectives.

10.5. Insurance
The organisation maintains an insurance policy with VMIA that insures the organisation against the risk of a financial (insurable) loss. Insurance for externally instigated fraud will all be maintained as appropriate including insurance against the theft of Institute property. Insurance coverage is reviewed on an annual basis.

---

11. MONITOR & REVIEW

The Fraud and Corruption Control Plan is subject to regular monitoring and review, to ensure fraud controls are implemented effectively achieving intended outcomes. Significant change within the organisation may trigger an update of the plan to ensure it contains accurate and up-to-date information.

---

12. CONTINUAL IMPROVEMENT

Through the monitor and review process of the fraud & corruption control plan the organisation will identify ways in which the plan, fraud and corruption control framework, policy and processes can be improved.

---

13. LEGISLATIVE REFERENCES

- Australian Standard Fraud and Corruption Control AS 8001-2008
- Australian Standard AS ISO 31000:2018 Risk Management: Guidelines
- Financial Management Act 1994
- Standing Directions of the Minister for Finance 2018
- Public Interest Disclosure Act 2013
- Privacy Act 1988