University of Otago
ŌTĀKOU WHAKAIHU WAKA

Fraud and Corruption Procedures

University Operations

Office of Risk, Assurance, and Compliance

Health, Safety and Wellbeing | Chief Operating Officer | Campus and Collegiate Life Services
Transformation and Improvement | Information Technology Services | Enterprise Project Management
Sustainability | Property and Campus Development | Divisional Services and Administration

Contents

1. PURPOSE

1.1 The purpose of the Fraud and Corruption Prevention Procedures ("Procedures") is to:

a. Provide clear guidance for the prevention, detection and overall response to potential or suspected instances of fraud and corruption ("Incident") within or involving the University of Otago ("UoO" or "University");

b. Outline the response and reporting methodology to be implemented upon the identification of a potential or suspected Incident, involving University Staff (defined in Section 6) or third parties (i.e., external parties such as clients, consultants, service providers or other members of the public);

c. Ensure that effective and timely action is taken in the event of the identification of an Incident; and,

d. Ensure opportunity is taken to strengthen controls to minimise and remedy harm caused by fraud and corruption.

1.2 These Procedures outline:

a. The scope and objectives of the Procedures;

b. The University's zero tolerance towards fraud and corruption;

c. How fraud and corruption are defined for the purposes of this Procedures and the University;

d. Clear roles and responsibilities for all University Staff in relation to fraud and corruption;

e. The University's key fraud and corruption prevention controls;

f. Reporting and investigation of suspected Incidents;

g. The consequences of a breach of these Procedures;

h. The monitoring of suspected and confirmed Incidents; and,

i. The planning and evaluation of desired strategies to combat Incidents.

1.3 These Procedures are to be read in conjunction with the University's:

a. Fraud and Corruption Policy

b. Ethical Behaviour Policy

c. Protected Disclosures Policy and Procedure

d. Conflict of Interest Policy

e. Financial Delegations Policy

f. Acceptance of Gifts, Benefits and Gratuities Policy

g. Externally Funded Research Policy – Applications for External Funds – Grants and Contracts

h. Guidelines for responsible practice in research and procedures for dealing with allegations of misconduct in research

i. Closure of commercial accounts and transferring surpluses

j. Intellectual Property Rights Policy

k. Intellectual Property Rights of Graduate Research Students Policy

2. SCOPE

2.1 These Procedures apply to all University Staff in relation to fraud and/or corruption, whether suspected, alleged or proven, that are either committed:

a. Against the University by a person or another organisation; or

b. By any University Staff against any third party (i.e., external parties such as clients, consultants, service providers or other members of the public).

2.2 These Procedures have been written to align with best practice standards including the Joint Australian and New Zealand Standards AS8001-202108 Fraud and Corruption Control and the OAG Discouraging Fraud and Integrity Services Framework 2022. The Office of Risk, Assurance and Compliance ("ORAC") is always available to assist you in applying these Procedures and the activities it promotes. Please contact the team directly (fraud@otago.ac.nz) if you have any questions or concerns.

3. OBJECTIVES

3.1 To reduce the risk of fraud or corruption within the University, the three key objectives that need to be met are:

a. **Prevention**: Reducing the risk of Incidents taking place within the University;

b. **Detection**: Scanning for and identifying potential Incidents early and providing effective channels for reporting; and

c. **Response**: Responding to Incidents in a robust, efficient and defensible manner, taking immediate action to remedy the harm caused, and addressing control weaknesses.

4. UNIVERSITY'S RESPONSE TO FRAUD AND CORRUPTION

4.1 The University is committed to preventing, detecting, and responding to fraud and/or corruption. As a public sector organisation that is entrusted with public funds, the University must set and maintain the highest standards of honesty, integrity, respect, and transparency. Allegations of fraud and corruption can cause serious reputational, cultural, legal, and financial harm for the University. Hence, all University Staff are expected to act in accordance with these high legal, ethical, and moral standards at all times.

4.2 Accordingly, the University adopts a zero tolerance in relation to fraud and corruption.

4.3 Zero tolerance within the University means:

a. All Incidents will be assessed and/or investigated, with appropriate action taken (in accordance with the University's Ethical Behaviour Policy);

b. All confirmed suspicions of fraud or corruption will be treated as serious misconduct and, where deemed appropriate (i.e., Significant incidences of fraud or corruption (defined in Section 6)), will be referred to the NZ Police, NZ Serious Fraud Office or any other appropriate regulatory and/or enforcement agency where applicable; and

c. Where deemed appropriate, the University will take all necessary measures to recover any loss or expenditure in relation to fraud or corruption activities. This includes, but is not limited to, recovery of intellectual property, crime and fidelity insurance cover, physical assets, money, third party expenses incurred and investigation costs.

5. FRAUD AND CORRUPTION CONDITIONS

5.1 The four generally recognised conditions for fraud and corruption to occur are:

a. **Opportunity:** The presence of an opportunity (e.g., poor internal controls);

b. **Motivation:** An incentivised/pressured individual motivated to behave unethically;

c. **Rationalisation:** Justification by the individual to undertake the activity); and,

d. **Capability:** Required characteristics, abilities, or skills to enable fraud and/or corruption.

5.2 These Procedures have been written to address these conditions within the University.

6. DEFINITIONS

Term	Definition
Assessment Team	For the purpose of these Procedures, the Assessment Team is an independent, objective group within UoO who is responsible for performing an initial assessment to determine the appropriate course of action.
Assets	These include, but are not limited to: • Cash and cash equivalents; • Financial assets (e.g., debtors, loans); • Property, plant and equipment; • Furniture and fittings; • ICT devices and equipment; • Collections; • Vehicles and other stock; • Intangible assets (e.g. computer software, licenses); and • Intellectual property of the University.
Bribery	A bribe means any money, valuable consideration, office, or employment, or any benefit, whether direct or indirect. 'Bribery' is the practice of offering something (a bribe) in order to gain an illicit advantage by altering the behaviour of the recipient.
Corruption	'Corruption' is defined as dishonest activity in which a person associated with an organisation acts contrary to the interests of the organisation and abuses their position of trust to achieve personal advantage or advantage for another person or organisation. Examples of corruption are provided in Section 7 below.
Decision maker	For the purpose of this document, the Decision Maker is the individual within UoO who is responsible for deciding: • whether the Person of Interest should be subject to disciplinary

	(or other) action; and • whether the University needs to refer the matter to any external authorities. The Decision Maker must be independent of the Investigation Team.
Due diligence	Comprehensive examination conducted on a business, individual, or process before engaging in an agreement. It serves as a means to ensure professional transparency and instil confidence by thoroughly vetting the involved parties and processes prior to entering into a transaction or agreement.
Error	There is a distinct divide between the definitions of the term 'fraud' and 'error'. Error refers to an unintentional act or omission, made unknowingly by an individual or group lacking in knowledge or oversight. Error may be an unintentional misstatement of information including the unintentional omission of an account or a disclosure; performing an action that created unexpected or unintentional outcomes or consequences. In contrast, 'fraud' is a deliberate act.
Fraud	'Fraud' is an intentional and dishonest act involving deception or misrepresentation, to obtain or potentially obtain an advantage for an individual or any other person. It includes the deliberate falsification, concealment, destruction or use of falsified documentation used or intended for use for a normal business purpose of the University or the improper use of information or position whether or not for personal benefit. Examples of fraud are provided in Section 7 below.
Fraud Control Officer	Designated role to support the Vice-Chancellor with the management of fraud and corruption risk. This is assigned to the Head of Risk, Assurance and Compliance. Key roles and responsibilities are defined in Section 8 below.
Incidents	Potential or suspected instances of fraud and corruption.
Informal Process	A preliminary, low-level response to a concern or allegation, aimed at clarifying facts and determining whether further action is required. It may involve discreet enquiries but does not constitute a formal investigation.
Investigation Team	For the purpose of these Procedures, the Investigation Team is a team of appropriately trained individuals with the necessary knowledge, skills and authority to conduct an investigation. This Team may include individuals from within UoO and external specialists ensuring they are appropriately licensed.
Kickback	A form of bribery in which an unofficial payment is received by a person in a position of authority or decision-making, for services rendered or awarding business.

Natural justice	'Natural justice' is defined as the duty to act fairly. It has two key aspects: • Fair process; and • Ensuring the decision maker is not biased. A fair process is one where the complaint is taken seriously, and where both parties are kept informed about the progress of any investigation. A fair process also requires that the Person of Interest be told about any allegations that have been made against them and have the opportunity to respond.
Notification	A 'notification' is a report or disclosure of suspected or actual incidents of fraud and corruption.
Person of Interest	For the purpose of this document, the Person of Interest is the individual(s) who is the subject of the investigation.
Preliminary Investigation	A structured fact-finding process to gather and assess initial evidence in order to determine whether a formal investigation is warranted. This process follows defined procedures to ensure confidentiality, impartiality, and proper evidence handling.

Serious Wrongdoing	Serious wrongdoing is defined (by the Protected Disclosure (Protection of Whistle-blowers) Act 2022) as any act, omission, or course of conduct in (or by) any organisation that is one or more of the following:
	• An offence;
	• A serious risk to:
	  o Public health; or
	  o Public safety; or
	  o The health or safety of any individual; or
	  o The environment
	• A serious risk to the maintenance of law, including:
	  o The prevention, investigation, and detection of offenders; or
	  o The right to a fair trial
	• An unlawful, a corrupt, or an irregular use of public funds or public resources;
	• Oppressive, unlawfully discriminatory, or grossly negligent, or that is gross mismanagement, and is done (or is an omission) by:
	  o University Staff;
	  o A person performing (or purporting to perform) a function or duty or exercising (or purporting to exercise) a power on behalf of a public sector organisation or the Government.

University	Refers to the University and, for risk oversight purposes, its subsidiaries

	and the Foundation Trust, to the extent that risks in those entities may materially affect the University's interests, obligations or objectives.
University Staff	For the purpose of these Procedures, 'University Staff' includes all: • Current and former University employees (casual, fixed term, permanent, part time and full time); • Persons with honorary or unpaid staff status at the University; • Agency employees and individuals seconded to the University; • University contractors (individuals, contractor staff, sub-contractors or persons affiliated with third parties) and consultants working with the university; and • Volunteers working for the University. Collectively, we refer to this group as "Staff". Any of these individuals are entitled and encouraged to make a disclosure.

7. EXAMPLES OF FRAUD AND CORRUPTION

7.1 Examples of **fraud** may include, but are not limited to:

a. Knowingly providing false, incomplete or misleading information to the University for unfair, unjustified or unlawful gain;

b. Forgery or alteration of documents or accounts belonging to the University;

c. Misappropriation or improper disposal of assets, including furniture, fixtures and equipment;

d. False invoicing/fake suppliers (creation of a fictitious invoice claiming payment for goods or services not delivered or exaggerating the value of goods delivered or services provided);

e. Cyber-attacks/ransomware;

f. Phishing attacks;

g. Academic fraud;

h. Theft of assets or inventory belonging to the University, even where deception is not used;

i. Theft of intellectual property or other confidential information, including student records;

j. Theft of cash, inventory or plant and equipment;

k. Accounts Receivable fraud (misappropriation or misdirection of remittances received by the University from a debtor including students);

l. Credit card or reimbursement fraud;

m. Financial reporting fraud (falsification of the financial statements with a view to obtaining some form of improper financial benefit);

n. Employment fraud, e.g., creating false employees, knowingly booking leave, or submitting false timesheets;

o. Purchasing activity which deliberately fails to follow the Procurement Policy and Procedures or seek the necessary approval such as false invoicing, bribes/kickbacks, split purchasing (to avoid

breaching approval limit), bid rigging;

p. Research grants and contracts – sub-contractors billing for work not performed, overcharging, absence of competitive bids for work;

q. Unauthorised use or misuse of the University facilities, vehicles or equipment; and,

r. Supporting others in, or in any way being part to, fraud, or not reporting fraud.

7.2 Examples of **corruption** may include, but are not limited to:

a. Any person who has a business involvement with the University, improperly using, or trying to improperly use, the knowledge, power, or resources of their position for personal gain or for the advantage of others;

b. Knowingly providing, assisting, or validating in providing false, misleading, incomplete or fictitious information to circumvent University procurement processes and procedures to avoid further scrutiny or reporting;

c. Disclosing private, confidential or proprietary information to outside parties without implied or expressed consent;

d. The provision or acceptance of cash, facilitation payments or kickbacks;

e. Payment or receipt of secret commissions (bribes), which may be paid in money or in some other form of value to the receiver and may relate to a specific decision or action by the receiver or generally (e.g., extravagant gifts and benefits paid to an employee);

f. Collusive tendering (the act of multiple tenderers for a particular contract colluding in preparation of their bids);

g. The improper use of a political/business position of authority or 'influence';

h. A conflict of interest involving a staff member who acts in his or her own self- interest rather than the interests of the University (e.g., failing to declare an interest in a transaction the University is about to enter into);

i. Manipulation of the procurement process by favouring one tenderer over others or selectively providing information to some tenderers. This frequently involves allowing tenderers to resubmit a 'non-complying' tender after being provided with the details of other bids;

j. Undisclosed gifts/donations or contributions/favours or entertainment intended to influence decisions (see Acceptance of Gifts, Benefits and Gratuities Policy); e.g., purchase without appropriate competitive process, academic grades, unduly influence University Staff recruitment; and,

k. Bribing officials (locally or in foreign jurisdictions) in order to secure a contract for the supply of goods or services, or in the recruitment of students.

8. ROLES AND RESPONSIBILITIES

Vice-Chancellor

8.1 The Vice-Chancellor has overall responsibility and accountability for the prevention and detection of fraud and corruption risk and responding to Incidents within the University.

8.2 The Vice-Chancellor may delegate responsibility for the implementation and maintenance of these Procedures to the Head of Risk, Assurance and Compliance and/or COO.

University Council

8.3 The University Council has overall responsibility and accountability for ensuring that appropriate governance mechanisms and corruption prevention procedures are in place and operating as designed.

Audit and Risk Committee

8.4 The Audit and Risk Committee ("ARC") is responsible for reviewing the University's Risk Management Framework and associated procedures for the effective identification and management of the University's financial and business risks, including fraud and corruption risks.

8.5 The ARC is responsible for overseeing the process of developing and implementing the Procedures, to provide assurance that the University has appropriate processes and systems in place to prevent, detect and effectively respond to fraud and corruption. Management is primarily responsible for fraud and corruption prevention and detection.

8.6 The ARC is also responsible for approving the Internal Audit Programme.

Financial Services

8.7 Financial Services is responsible for reviewing the insurance cover on an annual appropriate cover to the ARC for approval.

Senior Leadership

8.8 Senior leadership are responsible for role modelling high standards of ethical behaviour and setting the tone from the top on the University's zero-tolerance to fraud and corruption.

8.9 Senior leadership are responsible for developing efficient management controls, processes, training, and awareness regarding fraud and corruption, within their respective areas of responsibility.

8.10 If necessary, senior leadership shall seek assistance from and involve specialised resources such as Finance, Legal, Procurement or Risk, Assurance and Compliance, to ensure effective prevention, detection, and response to Incidents.

8.11 Within their respective business areas, all senior leaders must ensure that these Procedures are well understood and complied with.

8.12 All senior leadership must periodically communicate these Procedures both internally and externally with organisations that, or possibly will, hold a business relationship with the University.

Fraud Control Officer (Head of Risk, Assurance and Compliance)

8.13 Specifically, the Head of Risk, Assurance and Compliance (as the Fraud Control Officer) is responsible for:

a. Regularly monitoring these Procedures with updates made and communicated as possible;

b. Understanding and translating current best practice in fraud control into user-friendly practices and procedures;

c. Actively promoting a speak-up culture within the University, where Staff feel comfortable and are encouraged to report any suspected Incidents;

d. Delivering/coordinating training on relevant procedures, particularly to line management;

e. Developing systems to investigate and detect fraud;

f. Facilitating fraud and corruption risk assessments;

g. Being the point of contact for all fraud and corruption related concerns;

h. All reported allegations of fraud or corruption are assessed and/or investigated in a timely and appropriate manner;

i. Ensuring that all Incidents are reported to the Vice-Chancellor, Chief Operating Officer and Chief Financial Officer;

j. Leading investigations;

k. Maintaining and regularly reviewing the fraud register;

l. Ensuring that the University's annual Internal Audit Plan is developed and conducted in accordance with the provisions of The Professional Practices Framework (PPF) of the Institute of Internal Auditors; and,

m. Informing the University's external auditor (Audit New Zealand) and (if appropriate) the insurer of all suspected frauds.

Director of Human Resources

8.14 The Director of Human Resources is responsible for providing appropriate input and guidance as to the employment aspects of investigations to ensure people are treated fairly, in line with natural justice principles, and in accordance with the University's Disciplinary Framework.

8.15 The Director of Human Resources is responsible for determining what disciplinary procedures (if any) should occur, as a result of an investigation.

Line Managers

8.16 Line managers (Directors, Heads of Departments) are responsible for:

a. Role modelling high standards of compliance and ethical behaviour and setting the tone at the top on the University's zero-tolerance towards fraud and corruption;

b. Encouraging University Staff to attend fraud control training as appropriate and ensuring that University Staff are well trained;

c. Ensuring that all University Staff have a clear understanding of the Fraud and Corruption Policy, these Procedures, and their responsibilities regarding the prevention, detection and response to Incidents;

d. Developing and maintaining effective controls to prevent and detect Incidents in the University's regular business activities, as well as in specific programs or projects;

e. Ensuring that any weaknesses identified in established controls or procedures are reported to ORAC with recommendations for corrective action;

f. Actively promoting a culture of awareness, proactive detection and reporting of Incidents; and,

g. Ensuring that all University Staff who report Incidents are adequately supported and directed to the appropriate reporting channels.

All University Staff

8.17 All University Staff are responsible for:

a. Being aware of, and behaving in accordance with applicable laws, University policies, procedures and Ethical Behaviour Framework;

b. Acting with honesty, integrity and being opposed to all forms of fraud or corruption;

c. Remaining vigilant, immediately reporting any suspected or actual instances of fraud or corruption, whether from "internal" or "external" sources in accordance with the Section 10 below;

d. Participating in fraud and corruption awareness training offered by the University;

e. Adhering to the University's systems of internal control;

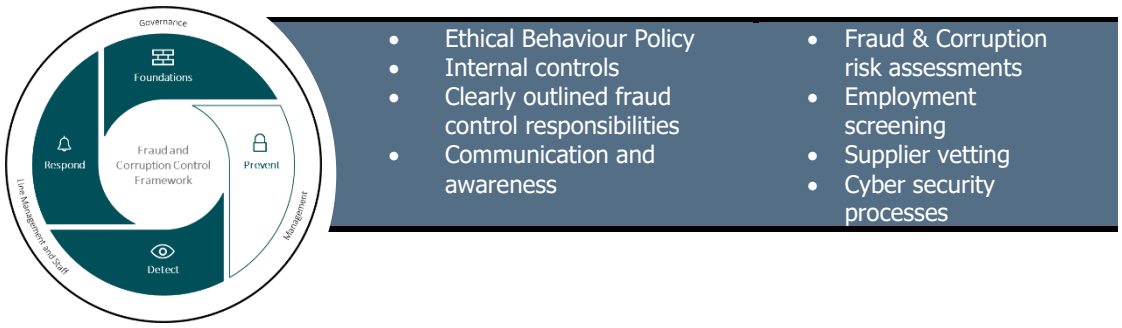
f. Not knowingly making a false or misleading report;

g. Co-operating with any investigation and assisting where needed (and not hindering or impeding an investigation);

h. Not conducting their own investigations of Incidents, unless assigned to do so by the unit or person in charge of investigations; and,

i. Confirming in writing, on a yearly basis, that they have complied with the Fraud and Corruption Policy and undertake to comply with this over the next 12 months.

9. PREVENT



9.1 The optimal way to reduce the risk of Incidents is through the implementation of effective prevention-focused business processes and internal controls supported by policies and procedures. These include, but are not limited to:

a. **Ethical Behaviour Policy:** Requiring all members of the University to be courteous, honest, fair, timely and ethical in their dealings;

b. **'Tone at the top':** Setting the 'tone at the top' through senior leadership by role-modelling and communicating the importance of ethical behaviour;

c. **Regularly reviewed Policy documentation:** Ensure all Policies and Procedures are appropriately in line with the changing fraud and corruption landscape;

d. **Separation of duties;** Assisting in detecting errors and deterring improper activities;

e. **Appropriate delegations and authorisation levels**: Ensuring University Staff strictly adhere to delegations of authority;

f. **Management of conflicts of interest:** Ensuring University Staff immediately notify their Head of Departments if they, directly or indirectly, hold any financial or other interest in an external organisation as a potential supplier;

g. **Clearly outlined fraud control responsibilities:** Communicating specific roles and responsibilities

for all University Staff fosters accountability and increases awareness of UoO expectations;

h. **Periodic communications:** Periodic communication of policies both internally and externally, particularly with consideration to time of the year such as during International Fraud Awareness Week in November;

i. **Raising awareness of the Procedures:** Potential awareness raising measures include regular newsletters, intranet, and email alerts;

j. **Adequate and regular fraud awareness training and supervision:** Regular training held to increase awareness of factors present for Incidents to occur, potential red flags, common and emerging fraud and corruption methods and University Staff roles in improving the fraud environment. Every three years, additional targeted training is delivered to those that have a significant role in preventing fraud;

k. **Fraud & corruption risk assessments:** In accordance with the AS 8001-2021 Fraud and Corruption Control Standards, conducted every three years through considering current processes and procedures, workshops and discussions and research into current fraud trends;

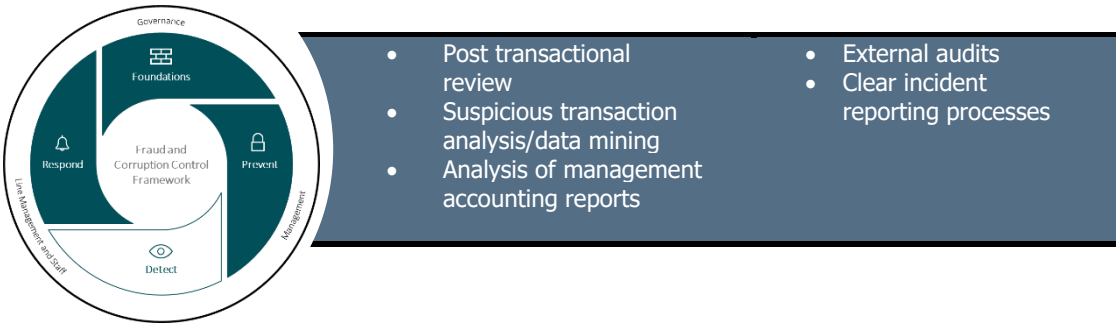
l. **Robust employment screening processes:** Completed at the discretion of the hiring manager, to prevent the employment of people with a history of dishonest conduct, including but not limited to, credit checks, conviction checks and referee checks;

m. **Supplier vetting processes:** Due diligence and continuous monitoring of new suppliers and customers by conducting bank account, telephone, trading address, IRD number verifications and completing media and Companies Register searches; and,

n. **Cyber security processes:** Continual maintenance and protection of the cyber security control environment as documented in the Cyber Security Framework. Noting that these Procedures do not cover cyber risk in any detail and that is responsibility of the Head of IT Assurance and Cyber Security.

9.2 The University's internal controls will be maintained and regularly reviewed by the Fraud Control Officer. Specific reviews of internal controls will be undertaken as part of the internal audit programme, along with ad hoc reviews as deemed appropriate by the University. Any weaknesses identified will be addressed on an ongoing basis.

10. DETECT



10.1 Detection strategies are the processes and controls designed to detect fraud after it has occurred. Detection activities include, but are not limited to:

a. **Post transactional review:** The identification of transactions or behaviours that may be

indicative of fraud, including, for example, creditors supplier master file reviews, PCard reviews, annual leave reviews and the review of high-risk journal types and expenses;

b. **Suspicious transaction analysis/data mining:** Annual suspicious transaction analysis, whereby a data mining process extracts the previous year's data for interrogation and investigation; and

c. **Analysis of management accounting reports:** monthly review of management accounts to remain alert for any unusual activities or trends which may reveal anomalies indicative of fraud. Some examples of the types of management accounting reports that can be utilised on a compare and contrast basis are:

   i. Financial reports detailing monthly performance against prior periods and budget;

   ii. Key performance indicator reports; and,

   iii. Reports comparing expenditure against industry benchmarks.

The External Auditor's Role in the Detection of Fraud

10.2 ORAC and the ARC will work with the External Auditor by:

a. Discussing the University's fraud environment and risk areas;

b. Discussing the audit procedures that will be carried out during the audit that are aimed at detecting material misstatements in the University's financial statements due to fraud or error;

c. Offering such assistance as the auditor may require to enable a more comprehensive examination of any issues;

d. Notifying the auditor on identified frauds; and,

e. The External Auditor is expected to notify ORAC and the ARC of any suspected instances of fraud, any identified fraud control risks and any weaknesses in internal controls that enhance the risk of fraud.

Making a notification (or disclosure)

10.3 All suspected instances of fraud or corruption must be reported immediately through (any one of) the following channels:

a. the Head of Risk, Assurance and Compliance,

b. the fraud email address or phone number provided below, which are monitored by the Office of Risk, Assurance and Compliance

   - Email: fraud@otago.ac.nz
   - Mobile: +64 27 4 359 808

c. the Vice-Chancellor,

d. the Chief Operating Officer,

e. the Chief Financial Officer,

f. the Director of Human Resources,

g. via a protected disclosure (in accordance with the Protected Disclosures Policy).

10.4 Notifications can be written or verbal. If verbal, the individual receiving the notification must record details of the notification in writing.

10.5 All University Staff who receive a notification of a suspected instance of fraud and/or corruption

are required to immediately notify the Head of Risk, Assurance and Compliance.

10.6 All reported Incidents will be reported by the Fraud Control Officer to the Chief Operating Officer, who will in turn inform the Chief Financial Officer, the Vice-Chancellor, and the Director of Human Resources unless a report involves (or may reasonably be regarded as having the potential to involve) one or more of those persons.

10.7 The Fraud Control Officer, in conjunction with the Chief Operating Officer, will notify the Chairperson of the ARC of all disclosures made.

10.8 Incidents of suspected fraud or corruption (as defined in Section 7) will be reported by the Fraud Control Officer as follows:

a. To the Chairperson of the ARC and Audit New Zealand within 48 hours; and,

b. To the ARC of the University Council at its next meeting or earlier if appropriate.

10.9 If the investigation has found reasonable grounds to indicate fraud or corruption has occurred, the Head of Risk Assurance and Compliance, in conjunction with the Chief Operating Officer, the Vice-Chancellor and the Chairperson of the Audit and Risk Committee will notify the Police, Serious Fraud Office, University's insurers, Audit New Zealand (on behalf of the Office of the Auditor General), Tertiary Education Commission and other external agencies as applicable.

Protected Disclosures

10.10 University Staff may instead make a protected disclosure, under the Protected Disclosures (Protection of Whistle-blowers) Act 2022, for instances of suspected Serious Wrongdoing by disclosing it, in accordance with the Protected Disclosures Policy, to any of the following persons at the University:

a. Their manager,

b. Their managers manager,

c. Any senior manager,

d. The Director of Human Resources,

e. The Office of Risk, Assurance and Compliance,

f. The Registrar,

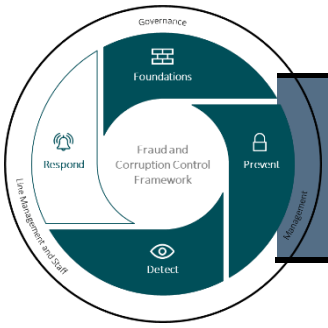
g. The Vice-Chancellor.

10.11 University Staff may choose to make a protected disclosure when they wish for the information that they provide to be kept confidential.

10.12 The identity of the person making a disclosure, and any details which may identify them, shall, if requested, be confidential to the extent provided for under the Protected Disclosures Policy.

10.13 Refer to the University's Protected Disclosures Policy for further details.

11. RESPOND (the "Fraud Response Plan")



- Investigation
- Processes aligned with natural justice
- Disciplinary Procedures
- External Reporting
- Insurance Protection

11.1 This section provides detail on the methodology for completing an assessment and/or investigation. It acts as a checklist of actions and a guide to follow in the event fraud or corruption is suspected.

11.2 This part of the process is performed when an Incident is considered by the Fraud Control Officer to be significant and warrants further assessment. In assessing whether the Incident is sufficiently significant to warrant further assessment and/or investigation, the Fraud Control Officer may consider various factors such as the following:

a. Estimated loss;

b. Nature of the allegations;

c. Reliability of the information; and

d. Individuals allegedly involved.

11.3 If it is determined that the Fraud Response Plan is to be used, then the Assessment and Investigation Teams (defined in Section 6) must ensure they:

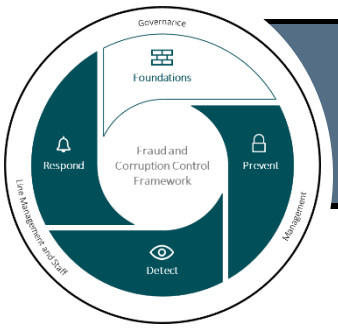
a. Apply the principles of natural justice (defined in Section 6);

b. Are familiar with the Fraud and Corruption procedures; and,

c. Are authorised by the Fraud Control Officer, to conduct an assessment or investigation of the Incident.

11.4 Full details of the Fraud Response Plan, including the Methodology to be followed, are outlined in **Appendix A**.

12. FOUNDATIONS



- Annual Review of Fraud Control Plan
- Internal Audit Plan
- Mitigation Strategy Review
- Policies and Regulations Review

12.1 The following section identifies the desired state of the planning, monitoring and evaluation strategies.

12.2 The Fraud Control Officer will maintain the register that records fraud or corruption reports and investigations in a secure file and will ensure compliance with the Privacy Act 2020 and related University policies.

12.3 The Fraud Control Officer will report to the Vice Chancellor and ARC quarterly on all Incidents. Reporting will be limited to the number of reports, with a high-level summary of outcomes (i.e., no further action taken, upheld or dismissed).

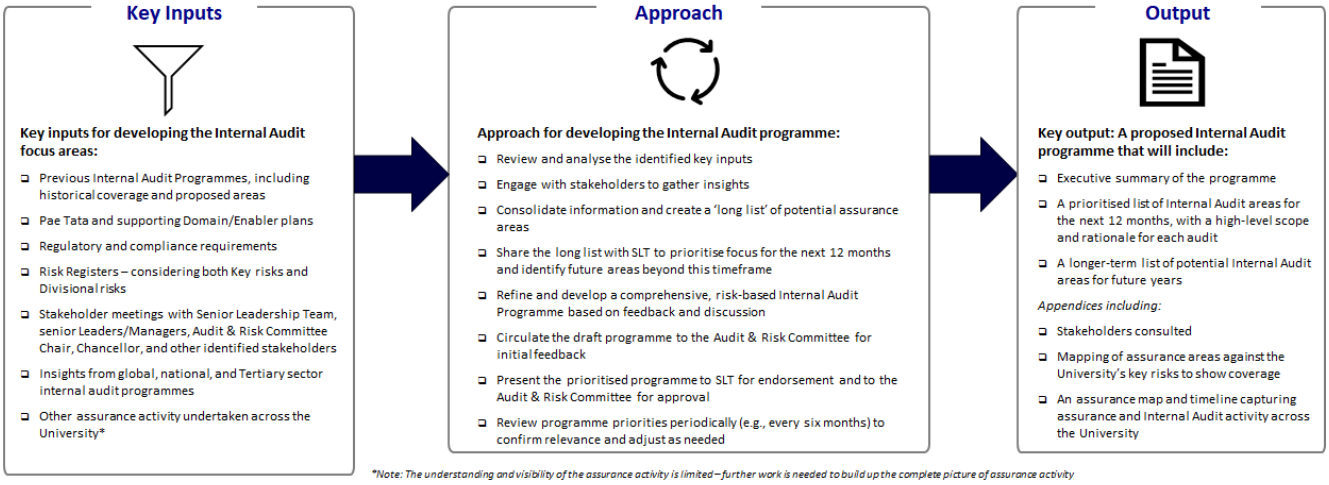
12.4 Where deemed necessary, the Fraud Control Officer will notify the Vice-Chancellor, the Chairperson of the ARC, and Audit New Zealand as soon as practicable.

12.5 The Fraud Control Officer, in consultation with the ORAC, will monitor and review the University's Policy and Procedures and recommend updates as required. In collaboration with the Audit and Risk Committee and the Council, these recommendations will be considered on a periodic basis.

The Internal Audit Programme

12.6 The Internal Audit programme is developed on a risk-weighted basis to address areas of critical concerns, including fraud and corruption risks.

12.7 It is developed in consultation with a wide range of internal stakeholders, and with reference to a range of key inputs, to ensure that it addresses the areas of highest risk, as detailed below.



APPENDIX A: DETAILED FRAUD RESPONSE PLAN

13. THE ASSESSMENT TEAM

13.1 The Assessment Team shall consist of relevant University Staff who are primarily responsible for the initial assessment of all Incidents:

Fraud Control Officer (Head of Risk, Assurance and Compliance) or delegate
Is responsible for *managing* fraud and corruption related Incidents, from when they are notified/identified.

Assessment Team

Director of Human Resources
Is responsible for provision of *HR oversight and/or advice* throughout the process.

Support Roles
(when necessary, as determined by the Fraud Control Officer)

Relevant Manager
Is responsible for providing relevant information to enable well-informed decision making and support the protection and preservation of evidence.

General Counsel
is responsible for the provision of legal oversight throughout the process, including managing the engagement of external legal advisors if required.

Chief Digital Officer or delegate
is responsible for supporting the protection and preservation of information systems and electronic evidence.

Vice-Chancellor
has an oversight role and holds overall responsibilities and accountability for responding to Incidents.

Chairperson of Audit and Risk Committee ("ARC")
has an oversight role (refer to 8.4 – 8.6.

13.2 The Assessment Team shall determine the appropriate course of action when fraud and/or corruption is suspected and identify the criteria or factors that shall assist in deciding whether the Incident is escalated into an investigation (refer to section 6).

14. POTENTIAL FOR CONFLICT OF INTEREST (POTENTIAL, ACTUAL OR PERCEIVED)

14.1 Where an individual listed as part of the Assessment Team or Support Roles (refer to the above diagram in 13.1) is the subject of the investigation or could be otherwise conflicted, they should

not be part of the investigation process.

14.2 Where necessary, an appropriate replacement will be used. If the Fraud Control Officer is implicated, the Vice Chancellor will be responsible for the investigation. If the Vice-Chancellor is implicated, the Chairperson of the ARC will hold that responsibility.

15. ENGAGING THIRD PARTIES

15.1 Where necessary, it may be appropriate to engage the services of appropriately experienced and qualified third parties (e.g. employment lawyers, forensic accountants, ICT and data analysts, fraud investigators or other subject matter experts) to support the Assessment Team. This will be done in accordance with the Procedures.

16. OTHER UNIVERSITY STAFF

16.1 Where required, other University Staff may be required to support the investigation. This will be determined by the Assessment Team outlined above and subject to clearing necessary conflict and independence checks.

17. FRAUD RESPONSE PLAN ROLES AND RESPONSIBILITIES

17.1 The specific role of the **Assessment Team** is to:

a. Conduct an assessment of the Incident to determine whether an investigation is warranted (or referral back to line management and/or Human Resources);

b. Assess risks present, both internally and externally;

c. If an investigation is warranted, decide on the nature of the investigation required on a case-by-case basis (scope, method, approach, and timeframe); and,

d. Maintain and update the Fraud Incident Response Checklist (see **Appendix A**) throughout the process (as required).

17.2 The specific role of the **Investigation Team** is to:

a. If an investigation is warranted, conduct an investigation of the Incident as per the nature decided by the Assessment Team; and,

b. Maintain and update the Fraud Incident Response Checklist (see **Appendix A**) throughout the process (as required).

17.3 The specific role of the **Fraud Control Officer** is to:

a. Advise the Vice-Chancellor that an Incident has been reported;

b. Notify insurers (if required) and clarify any requirements the insurer may have;

c. Appoint the Assessment Team based on the nature of the Incident;

d. Determine whether an external specialist or specialists (e.g., employment lawyers, forensic accountants, ICT and data analysts, fraud investigators or other subject matter experts) should be consulted or involved;

e. Notify relevant external authorities in accordance with the Policy and Procedures;

f. Decide who the Lead Investigator will be;

g. Oversee the assessment and investigation of the Incident; and,

h. Monitor progress and communicate as appropriate in accordance with the Procedures.

17.4 The role of the **Director of Human Resources** is to:

a. Provide appropriate input and guidance into the employment element of the investigation, to ensure that all people are treated fairly, in line with natural justice principles, and in accordance with the University's Disciplinary Policy; and

b. Determine what disciplinary action (if any) should occur, following an investigation.

17.5 There are a number of roles that may be asked to **support** the Assessment Team or be involved in an investigation. These can include but are not limited to:

a. General Counsel – providing specialist legal advice to the Assessment Team and Investigation Team during the course of the assessment and investigation;

b. Chief Digital Officer (or delegate) – working with the Assessment and Investigation Teams to ensure electronic evidence is identified, collected, extracted, preserved, analysed and stored with consideration for confidentiality and legal process;

c. Relevant Manager – if appropriate, the relevant Manager of the area an alleged incident has occurred, will be informed of the allegations and may be involved in the investigation;

d. Chairperson of ARC– is notified of all reported Incidents. They will be involved in the decision to notify external authorities; and,

e. Vice-Chancellor – is notified of all reported Incidents. If, after an initial assessment, an investigation commences, the Vice-Chancellor will have an oversight role. They will be involved in the decision to notify external authorities.

18. FRAUD AND CORRUPTION INCIDENT RESPONSE CHECKLIST

18.1 Refer to a summary of the fraud incident response steps in **Appendix B**. The Assessment and Investigation Teams should use the checklist as a guide when responding to Incidents. It should be updated regularly throughout the stages of response.

19. METHODOLOGY

19.1 The following four stage process is a principles-based methodology which can be applied to any type of incident. Each of the four stages are outlined in this document with:

a. Suggested steps to consider completing;

b. Who should typically perform each step; and,

c. Key considerations when completing each stage of the process.

19.2 The methodology is to be considered in the context of the circumstances. In some cases, particular steps may not be required.

20. STAGE 1: INITIAL ASSESSMENT

Objective: To understand what is known so far, so that decisions can be made about what next steps (if any) should be taken.

Note: This stage should be completed within 3 days of the Incident being reported.

Assemble the Assessment Team

20.1 When an Incident is reported, the Fraud Control Officer shall:

a. Consider the need for an urgent response (e.g., risk to life or harm to people, flight risk, protection of discloser (see below), securing potential evidence, freezing orders to reduce risk of dissipation of assets);

b. Notify the Chief Operating Officer, who will in turn inform the Chief Financial Officer, Vice-Chancellor and Director of Human Resources in a timely manner;

c. Where deemed necessary, notify the Chairperson of the ARC within 48 hours, and report to the ARC of the University Council at its next meeting, or earlier if appropriate;

d. Identify the members of the Assessment Team;

e. Coordinate the activities of the Assessment Team;

f. Ensure risks (including conflicts of interest) are identified, managed and documented; and,

g. Update the Fraud Incident Register with:

i. Date and time the Incident was reported;

ii. Date and time the Incident was detected;

iii. How the Incident came to the attention of the Fraud Control Officer;

iv. The nature of the Incident;

v. Estimated value of loss (if any) to the University; and,

vi. The action taken following discovery of the Incident.

20.2 If the Incident was reported via a protected disclosure, refer to the Protected Disclosures Policy for the required process.

Triage current information

20.3 An initial assessment must be made by the Assessment Team, to determine whether there are reasonable grounds for concern, and to identify the steps that are necessary to appropriately respond to the alleged Incident.

20.4 This assessment should be managed efficiently and, where possible, be completed within 3 days after the Incident is reported.

20.5 This assessment should seek to understand:

a. The University Staff who is/are alleged to have acted wrongly (i.e., the Person(s) of Interest);

b. The alleged breaches in relation to University policy, procedures, and/or external laws and regulations;

c. The existence of any related investigations;

d. The reliability of the information provided about the Incident;

e. The risk of ongoing harm, loss or damage and whether the alleged activity could be continuing;

f. The need for supporting information or potential evidence to be secured;

g. The need to contact relevant authorities (e.g., NZ Police, Serious Fraud Office, Audit New Zealand); and

h. Any special considerations (e.g., union issues, mental health and wellbeing of University Staff, anonymity of the discloser, the need to involve law enforcement, the involvement of the media).

20.6 With this information, the Assessment Team should understand the context of the Incident, and determine the appropriate response, being, whether it is:

a. Investigated under the methodology as set out in this document;

b. Treated as misconduct and dealt with under the Ethical Behaviour Policy; or

c. Treated as an operational incident and therefore managed by the appropriate Line Manager.

20.7 The reasons for this decision must be documented. All records should be stored in a secure electronic and/or physical file location, accessible only by the Assessment Team and the Vice-Chancellor to protect confidentiality.

20.8 If the Assessment Team decides an investigation is not required, move to the Reporting stage.

20.9 If the Assessment Team decides an investigation is required, proceed with an Investigation (as outlined in section 21 below).

Identify Lead Investigator

20.10 If the Assessment Team decides an investigation is required, the Fraud Control Officer will be the Lead Investigator. However, the Fraud Control Officer may delegate the investigation to another appropriate investigator at their discretion in accordance with section 17.3(f) of the Procedures.

20.11 The Investigation Team will be made up of the Lead Investigator and the members of the Assessment Team deemed appropriate by the Fraud Control Officer, alongside any other individual the Fraud Control Officer deems appropriate.

20.12 Note: Those undertaking an investigation must be appropriately trained, independent, have the necessary knowledge, skills and appropriate University position of authority to ensure the investigation is conducted fairly, transparently and in line with all University privacy, employment and disciplinary procedures.

20.13 The Fraud Control Officer must consider the need to engage external specialists to assist or lead an investigation. These external specialists may include, but are not limited to:

a. Employment lawyers;

b. Forensic accountants;

c. ICT and data analysts;

d. Fraud investigators; or

e. Other specialist subject matter experts.

20.14 Note: If legal privilege may apply, external specialists should be engaged by General Counsel instead of the Fraud Control Officer.

Notify relevant parties

20.15 If the Assessment Team has found reasonable grounds to indicate fraud or corruption has occurred, the Fraud Control Officer, in conjunction with the Vice-Chancellor and the Chairperson of the ARC will notify the Police, Serious Fraud Office, Audit New Zealand (on behalf of the Office of the Auditor General) and other external agencies as applicable.

20.16 The Fraud Control Office should also notify insurers (if required) and clarify any requirements the insurer may have.

Protect the rights of University Staff

20.17 The Lead Investigator should seek advice from the Director of Human Resources before approaching University Staff with an allegation of fraud or corruption, conducting interviews, and when agreeing disciplinary actions.

20.18 The Director of Human Resources and General Counsel should also consider whether specialist employment law advice is required.

20.19 When a decision has been made by the Assessment Team to undertake an investigation, the Lead Investigator, in conjunction with the Director of Human Resources and General Counsel / or a Legal Advisor (regarding managing the risks that apply to premature notification), must firstly:

a. Inform in writing, the Person(s) of Interest, and provide an overview of the allegation, witnesses and evidence gathered to date supporting the allegation;

b. Advise the Person(s) of Interest in writing of the expected investigation process, including whether a disciplinary process may result;

c. Request a meeting with them and, if they wish, invite them to bring a representative or support person(s). If the representative is of a legal nature, the Lead Investigator will attend the meeting with the General Counsel;

d. Meet with the Person(s) of Interest and their representatives to explain the allegations;

e. Request a written response to the allegations within a reasonable time period (if verbal, these must be documented);

f. Make sure the Person of Interest is aware of their rights as an employee of UoO; and

g. Fully consider any explanation received from the Person(s) of Interest before conclusions are made.

21. STAGE 2: INVESTIGATION

Objective: To collate information in a sound manner and undertake analysis to enable an informed conclusion to be made.

Plan the investigation

21.1 A case file should be created by the Investigation Team. This will be the formal record of the investigation and will remain confidential. The case file should include the following relevant sections:

a. Investigation Plan;

b. Communication Plan;

c. Interview notes and other notes;

d. Supporting documents identified; and,

e. Final report.

21.2 The Lead Investigator will determine where the case file will be saved, and who will have edit and read-only access.

21.3 The Lead Investigator, in conjunction with the Investigation Team, is responsible for documenting an Investigation Plan. The Investigation Plan should outline:

a. Objectives of the investigation;

b. Scope of the investigation (including period of data/evidence for review);

c. A chronology of the facts known, and allegations made;

d. Assessment and documentation of the issues;

e. Background information of subject matter knowledge required;

f. Identification of who holds potentially relevant information; and,

g. Key phases and activities planned to be completed throughout the investigation with responsible University Staff and timeframes (e.g., interviews, analysis, completion of case file).

21.4 Note: The Lead Investigator should consider whether the investigation plan should be documented in a terms of reference ("TOR").

21.5 A TOR is a document that aims to ensure the parties involved in an investigation understand its scope and legal and natural justice requirements. A TOR may include the following sections:

a. Scope;

b. Investigator;

c. Role of investigator;

d. Investigation process;

e. Natural justice;

f. Notifying the person / persons of interest;

g. Interviews;

h. Investigation report;

i. Privacy and confidentiality;

j. Legal privilege (if applicable);

k. Support available;

l. Timetable; and,

m. Contact person.

21.6 A Communication Plan should also be created by the Investigation Team. This should:

a. Include a list of persons entitled to know about the investigation and related activities (e.g., discloser, Vice-Chancellor, Audit New Zealand, NZ Police, Tertiary Education Commission, or Serious Fraud Office);

b. Establish the nature, method and frequency for any ongoing communications and who will be responsible for each; and,

c. Consider any other individuals who may already be aware of the Incident, and whether any further communication is required.

Record keeping

21.7 The Lead Investigator is required to maintain a full record of any investigation taken, including, but not limited to:

a. Details of the allegation(s) such as suspected activity, timeframes, details of University Staff or third parties involved (recognising the privacy of any Protected Disclosure made);

b. Comprehensive notes, recordings and/or transcripts of all conversations, discussions, meetings and interviews (including date and time, location, attendee names, positions and outcomes);

c. Forensic copies of all relevant digital communications (e.g. emails, chat);

d. Forensic copies of all documents reviewed or reports/data extraction;

e. Detail of disciplinary action taken; and,

f. Records of any tests and analyses undertaken.

21.8 Potential evidence must be protected and all reasonable steps taken to ensure it is not contaminated, lost or destroyed. No evidence should be altered in any way.

21.9 All documents (originals and working papers) should be circulated and stored in a manner that has been agreed with General Counsel. Documents should be stored in a secure place, be free from tampering/damage and follow privilege requirements, where applicable.

21.10 Document circulation should be minimised to only what is necessary and always password protected.

Prevent further loss and secure evidence

21.11 The Investigation Team must take steps to protect UoO from any further losses and secure any potentially relevant evidence (see paragraph 21.14 below).

21.12 Prior to taking action, the Investigation Team should seek guidance from General Counsel,

Human Resources and IT/Privacy as required. Consideration should be given to legal, regulatory, privilege, privacy and confidentiality requirements when identifying and gathering potential evidence. The principles of natural justice should be balanced with the risk of evidence tampering and destruction.

21.13 Consideration should also be given to the impact of these actions on the mental health and wellbeing of University Staff. The Investigation Team should seek to minimise any impact and refer to available support where necessary.

21.14 Potential steps may include one or more of the following:

a. Preservation of any documents, electronic evidence, external hard drives or personal drives;

b. Applying for and executing civil freezing or search orders;

c. Suspending the Person of Interest's IT access rights for University systems and software;

d. Restricting the Person of Interest's business duties, responsibilities and activities;

e. Removing or restricting physical access to University premises for the Person of Interest;

f. Cancelling credit cards, fuel cards and other purchase cards of the Person of Interest;

g. Removing and securing mobile phones and other mobile devices (e.g., laptops and tablets). This should include obtaining any passwords and chargers for the devices. The device should be set to airplane mode and then switched off;

h. Consideration of the Person of Interest's flight risk, potential for misconduct or malicious behaviour; and,

i. Consideration of the need to conduct any relevant searches (e.g., emails, phone, locker or other physical workspace).

21.15 Remember: Any evidence must be collected in a forensically sound manner, meaning that all files are properly collected and corresponding metadata (dates, file paths, host) have been saved and not altered during the process.

21.16 A Chain of Custody Form must be used to record the initial collection, ongoing safekeeping and any movements/transfer of the items.

Gather documents

21.17 The Investigation Team should consider the need to conduct a scene examination which may involve documenting, photographing and recording detailed records/diagrams.

21.18 The Investigation Team should obtain copies of internal policies, procedures, laws and/or external regulations and other requirements that are alleged to have been breached.

21.19 The Investigation Team should consider any other documents that may be relevant to the investigation.

Fact finding and interviews

21.20 The Investigation Team should undertake activities to understand the extent of the Incident and inform any findings.

21.21 Prior to taking action, the Investigation Team should seek guidance from General Council, Human Resources and IT/Privacy as required.

21.22 Fact finding activities may include (but are not limited to) any of the following:

a. Forensically processing, reviewing and collating physical and electronic documentation;

b. Interviewing relevant University Staff or external parties, where appropriate, including obtaining written, signed statements;

c. Forensic examination of University email accounts, messaging, telephone and mobile phone records;

d. Forensic examination of computer systems, networks, cloud storage and SaaS access, backup tapes;

e. Forensic examination of relevant hard copy records;

f. Data analytics and visualisation;

g. Collection of printer logs;

h. Collection of building or site access records and swipe card logs;

i. Collection of CCTV footage;

j. Enquiries with banks and other financial institutions;

k. Reviewing employment files (as appropriate);

l. Review and analysis of credit cards (including any Purchase Cards) and banking or financial activities, delegations or processes;

m. Enquiries with other third parties including contractors, businesses or service providers; and,

n. Tracing funds, assets, goods lifecycles.

21.23 When conducting any interview as part of the investigation, an interview plan should be drafted by one of the Investigation Team and reviewed by the Lead Investigator. The interview plan should consider:

a. The identified issues;

b. Documents that have been collected to date;

c. The parties involved;

d. Any external implications e.g., government reporting regulators, financial reporting, law enforcement, press and publicity, etc.);

e. Familiarisation of all the relevant information;

f. Understanding the interviewee (e.g., background, personal interest in the matter and reputation); and,

g. Relevant questioning to be asked.

21.24 Interviews should adhere to the core principles of sound investigative interviewing, following the P.E.A.C.E Interviewing Model. This includes:

a. Planning - Create a thorough interview plan (as outlined above);

b. Engage and explain - Establish rapport, provide context and outline the interview procedures;

c. Account - Obtain the interviewee's full account of events prior to asking follow-up questions. When questioning, use simple words and use open questions. Summarise the interviewee's account periodically to ensure correct understanding;

d. Closure - Review and summarise the interviewee's account, verify key aspects of interview have been sufficiently covered and explain the next steps from the interview; and

e. Evaluation - Review the information obtained in the interview.

21.25 The Investigation Team should also consider the following key points:

a. The need to seek guidance from General Counsel or Human Resources prior to inviting the interviewee and conducting the interview;

b. The interviewee should be given advance notice of the interview;

c. When interviewing the Person of Interest, they must be given the relevant information collected to date prior to the interview;

d. The interviewer and interviewees privacy and safety should be considered when determining the location of the interview;

e. There should always be two interviewers, one to lead the interview and the other to take notes;

f. Interviewees must be given the opportunity to be accompanied by a relevant support person(s) of their choice;

g. Interviews should be conducted in an appropriate location (e.g., private location free from distractions, away from workspace, accessible to the interviewee and interviewer);

h. Interviews should be recorded (with the permission of the interviewee);

i. Interviews should be conducted in accordance with natural justice principles; and

j. If there are multiple interviewees, interviews should be held in quick succession to minimise time between interviews. This minimises the time that individuals might speak to each other about the nature of the interview.

21.26 All evidence collected will need to be reviewed and considered in an objective manner. This includes hardcopy, electronic and human sources (e.g., witness interviews).

Analyse information gathered

21.27 The Investigation Team must determine if there is sufficient factual evidence for the Decision Maker to reach findings on whether:

a. The Incident occurred;

b. Any University policies and procedures were breached; and/or

c. Potential criminal activity under the Crimes Act 1961 or the Secret Commissions Act 1910 has occurred.

21.28 The Investigation Team should examine evidence gathered during the investigation and consider whether:

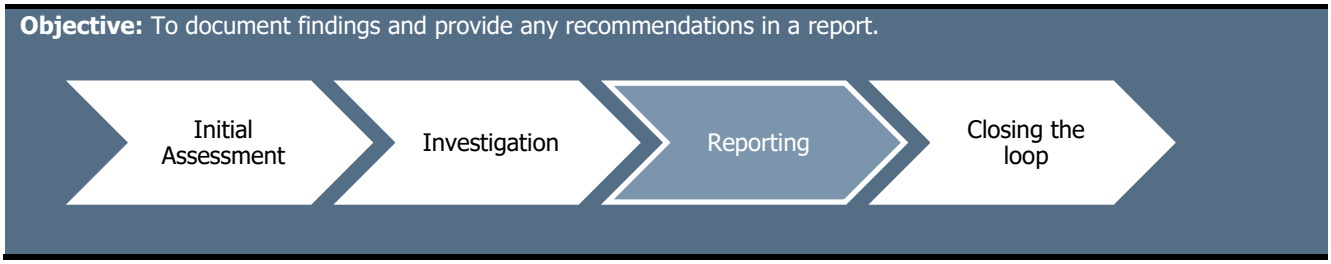
a. There is anything missing;

b. Any conflicts or contradictions exist;

c. Evidence is of adequate clarity, detail and logic; and,

d. There is a need to re-interview or confirm any details.

22. STAGE 3: REPORTING



Draft investigation report

22.1 An investigation report is required at the end of every investigation and must demonstrate that there has been a professional, thorough, transparent and fair investigation process. At a minimum, the report shall:

a. Confirm the Investigation Team and any other Staff involved and any use of external specialists;

b. Include an outline of the key aspects of the investigation and communication plan;

c. Address each concern or issue raised; and

d. Clearly communicate all findings and the reasons for them, referencing the information relied on in order to present decision-makers with sufficient facts to make a finding as to whether an allegation is founded or not.

22.2 An additional separate report shall be written which highlights any internal processes and/or internal controls that may need attention as a result with supporting recommendations/actions to consider.

22.3 Remember: This report could be subject to downstream scrutiny or be released under an Official Information Act request. It should be factual and not contain opinion.

Review the Draft investigation report

22.4 When reviewing the draft report, consider the following key points:

a. Covers key issues only;

b. The key issues are dealt with clearly and validated with supporting documentation / information within the report;

c. Steps taken and associated findings in the report are reasonable and in line with the scope and/or terms of reference;

d. Adheres to the principles of natural justice and is balanced; and,

e. Does not contain emotion, personal opinion, show judgment or pre-determination of guilt.

22.5 Before any other party, the draft report **must** first be shared with the Person of Interest to give them an opportunity to respond. A reasonable time (a minimum of 5 working days) should be allocated to the Person of Interest to provide their response.

22.6 Where necessary, the draft report should be updated based on this response prior to finalisation.

22.7 Where the Fraud Control Officer is not the Lead Investigator, the Investigation Team shall also provide the draft report to the Fraud Control Officer.

Share Final Report

22.8 The Lead Investigator will determine who should receive a copy of the report. This could include, but is not limited to:

a. Person(s) of Interest;

b. Decision Maker(s);

c. Assessment Team;

d. Human Resources;

e. General Counsel

f. Vice Chancellor;

g. Chief Operating Officer;

h. Chief Financial Officer;

i. ARC;

j. Tertiary Education Commission;

k. Serious Fraud Office; and,

l. Office of the Auditor-General / Audit New Zealand.

Consider disciplinary (or other) action

22.9 The Decision Maker will decide whether the Incident constitutes a breach of University policies.

22.10 If the Incident does constitute fraud, corruption, and/or a breach of University policies, the Decision Maker must refer the matter to the Director of Human Resources for consideration of disciplinary (or other) action. The Director of Human Resources is responsible for determining if any potential disciplinary action should follow the investigation, in accordance with the Ethical Behaviour Policy.

22.11 Any disciplinary actions taken against the subject of the investigation should also be fully documented and securely stored.

22.12 If the Incident does not constitute fraud, corruption and/or a breach of University policies, the Decision Maker must refer the matter to the Relevant Manager.

23. STAGE 4: CLOSING THE LOOP

Objective: To provide necessary updates to the discloser and other relevant parties at the conclusion at the investigation and consider lessons learnt.

Refer the outcome to third parties

23.1 Where appropriate, the outcome of the investigation (likely via sharing the report) may need to be referred to the following parties:

a. Fraud Control Officer (where delegate investigator used);

b. UoO's insurer;

c. Professional bodies;

d. Unions;

e. Audit New Zealand;

f. Tertiary Education Commission;

g. Serious Fraud Office; and,

h. NZ Police.

Reports to Law Enforcement Agencies
At a minimum, the following items should be provided to the law enforcement agency:

- A summary of the allegations;
- A list of witnesses and potential witnesses;
- A list of suspects and potential suspects;
- Copies of all statements obtained;
- A copy of the transcript of any interviews conducted;
- A copy of the recording of any interviews conducted;
- Copies of all documentary evidence obtained (the University should retain original copies in the event law enforcement request them);
- Any charts or diagrammatical summaries of the allegations and evidence that the University may have produced.

Update discloser

23.2 If the Incident was reported via a Protected Disclosure, the Lead Investigator must provide an update to the Discloser at the conclusion of the investigation in accordance with the Protected Disclosures Policy.

23.3 Subject to legal constraints, University Staff who report an Incident will be informed of the outcome of the investigation.

23.4 The details of an investigation must not be disclosed or discussed with anyone other than those who have a legitimate need to know or are directly involved in the investigation.

Close case file

23.5 At the conclusion of the investigation, the Lead Investigator must ensure the case file is up-to-date, complete and saved electronically with the appropriate restricted access.

Communications

23.6 The Fraud Control Officer, in conjunction with the Vice-Chancellor, Manager Communications Advisory Service and the Director of Human Resources, should be engaged in any internal communications to ensure an appropriate strategy is adopted.

23.7 The communication strategy should also consider whether other external stakeholders should be informed, including members of the public and the media. Any media queries that arise will be dealt with by the Vice Chancellor, in consultation with the Fraud Control Officer, General Counsel and the Director of Human Resources.

Recover losses

23.8 UoO will take all appropriate measures to recover any loss or expenditure attributable to fraud or corruption. This includes, but is not limited to recovery of intellectual property, physical assets, money, third party expenses incurred and investigation costs.

23.9 The Fraud Control Officer should consult with the General Counsel in relation to:

a. The requirement for an asset recovery specialist; and

b. Any need to claim from insurers.

Consider lessons learnt

23.10 At the conclusion of the investigation, the Fraud Control Officer should update the Incident register and review the reasons for the Incident to identify any existing gaps or exposure at the University, including assessing the adequacy of the internal control environment (particularly those controls directly impacting on the fraud incident and potentially allowing it to occur). The Fraud Control Officer is responsible for determining what (if any) measures are needed to prevent and/or detect a recurrence and strengthen future responses to fraud and corruption.

23.11 The Fraud Control Officer should also consider the need for any updates to the University's Policy and Procedures.

Maintaining Adequate Insurance Cover

23.12 The University maintains adequate insurance to cover for significant loss due to fraud.

23.13 Financial Services reviews the insurance cover on an annual basis and recommends appropriate cover to the Audit & Risk Committee for approval.

APPENDIX B: FRAUD/CORRUPTION INCIDENT RESPONSE CHECKLIST

Incident reference:

Person of Interest:

Lead Investigator:

Relevant Line Manager:

Key actions / dates *This is a summary of the key actions that should be completed throughout the four-stage process.*			
Action	**Date completed**	**Completed by**	**Details / Notes / Reference / Actions**
Incident reported		Discloser	
Initial assessment completed		Assessment Team	
Notification to Human Resources (if applicable)		Fraud Control Officer	
Notification to Vice-Chancellor / COO / CFO (if applicable)		Fraud Control Officer	
Draft report		Investigation Team	
Final report		Lead Investigator	
Referral to external authority		Decision Maker	
Outcome notified to discloser		Lead Investigator	
Outcome notified to Person of Interest		Human Resources	
Investigation / file closed		Lead Investigator	

Third party assistance (*if applicable*)	
External specialists	**Contact information**
Investigator / Forensic specialist	
External legal advisors	
Other specialist(s) (detail roles)	

Stage 1: Initial Assessment							
Case Name:							
Action	**Ref to Fraud Response Plan**	**Yes**	**No**	**N/A**	**Date completed**	**Completed by**	**Details / Notes / Reference / Actions**
Assemble the Assessment Team							
Is an urgent response required? *(e.g., threat/danger to person or property?)*	20	☐	☐	☐		Fraud Control Officer	
Is it a Protected Disclosure?	20	☐	☐	☐		Fraud Control Officer	
		☐	☐	☐			

If yes, process for Protected Disclosures followed per PP200-205?							
Vice-Chancellor notified?	20	☐	☐	☐		Fraud Control Officer	
Director of Human Resources notified?	20	☐	☐	☐		Fraud Control Officer	
Notification involves '*serious wrongdoing*'?'	20	☐	☐	☐		Fraud Control Officer	
If so, Chair of Audit and Risk Committee notified?		☐	☐	☐			
Assessment Team notified and assembled including Decision Maker?	20	☐	☐	☐		Fraud Control Officer	Assessment Team: Decision Maker:
Risks identified and managed (e.g., conflicts, wellbeing, legal, confidentiality)?	20	☐	☐	☐		Fraud Control Officer	Risks:
Triage current information							
Initial assessment complete and decision re investigation made and documented?	20	☐	☐	☐		Assessment Team	[If no investigation necessary, move to reporting stage]
Identify Lead Investigator							
Lead Investigator and Investigation Team identified?	20	☐	☐	☐		Fraud Control Officer	Lead Investigator: Investigation Team:
External specialists engaged (where appropriate)?	20	☐	☐	☐		Fraud Control Officer	Specialists engaged:
Notify relevant parties							
Police notified (where appropriate)?	21	☐	☐	☐		Fraud Control Officer	
Serious Fraud Office notified (where appropriate)?	21	☐	☐	☐		Fraud Control Officer	
Audit New Zealand notified (where appropriate)?	21	☐	☐	☐		Fraud Control Officer	
Other external authority (where appropriate)?	21	☐	☐	☐		Fraud Control Officer	Authority notified:
Insurers notified (where appropriate)?	21	☐	☐	☐		Fraud Control Officer	

Protect the rights of University Staff							
Advice sought from Human Resources prior to contacting Person of Interest?	20	☐	☐	☐		Lead Investigator	HR person responsible:
Person of Interest informed in writing?	20	☐	☐	☐		Lead Investigator	
Meeting requested with Person of Interest?	20	☐	☐	☐		Lead Investigator	
Response from Person of Interest received?	20	☐	☐	☐		Lead Investigator	

Stage 2: Investigation							
Case Name:							
Actions	**Ref to Fraud Response Plan**	**Yes**	**No**	**N/A**	**Date completed**	**Completed by**	**Details / Notes / Reference / Actions**
Plan the investigation							
Case file created and made secure?	21	☐	☐	☐		Investigation Team	Individuals with access to case file:
Determined period of data / evidence to obtain for review?	21	☐	☐	☐		Investigation Team	Review period:
Investigation Plan complete and saved to case file?	21	☐	☐	☐		Investigation Team	
Communication Plan complete and saved to case file?	21	☐	☐	☐		Investigation Team	Key contacts during investigation:
Record keeping							
All investigation team members informed of record keeping requirements?	21	☐	☐	☐		Lead Investigator	
Prevent further loss and secure evidence							
Guidance sought from Legal (if required)?	21	☐	☐	☐		Investigation Team	
Guidance sought from Human Resources (if required)?	21	☐	☐	☐		Investigation Team	

Considered the sources of evidence required and applicable to the Incident?	21	☐	☐	☐		Investigation Team	Document sources of evidence to collect and location: Other sources:
Sources of electronic evidence identified?	21	☐	☐	☐		Investigation Team	Document sources of evidence to collect, location and decisions made about collection: Other sources:
Gather documents							
Consider documents needed?	21	☐	☐	☐		Investigation Team	
Internal policies/procedures?		☐	☐	☐		Investigation Team	
Legislation?		☐	☐	☐		Investigation Team	
External regulations?		☐	☐	☐		Investigation Team	
Fact finding and interviews							
Guidance sought from Legal (if required)?	21	☐	☐	☐		Investigation Team	
Guidance sought from Human Resources (if required)?	21	☐	☐	☐		Investigation Team	
Guidance sought from IT and Privacy (if required)?	21	☐	☐	☐		Investigation Team	
Interview plan(s) complete? *(e.g., purpose of interview, objective of interview, order of interviews, who to conduct interviews, when and where interviews should take place etc.)*	21	☐	☐	☐		Investigation Team	Interviewees/ interview details:
Person of Interest provided with relevant information collected to date prior to interview?	21	☐	☐	☐		Investigation Team	
Interviews complete?	21	☐	☐	☐		Investigation Team	
Analyse information gathered							
Conclusion reached: sufficient evidence	21	☐	☐	☐		Investigation Team	Conclusion:

identified to support allegation?							
Further steps required (e.g., credit check, criminal check, other specialist advice)?	21	☐	☐	☐		Investigation Team	Further steps:

Stage 3: Reporting							
Case Name:							
Action	**Ref to Fraud Response Plan**	**Yes**	**No**	**N/A**	**Date completed**	**Completed by**	**Details / Notes / Reference / Actions**
Draft investigation report							
Investigation Report drafted?	22	☐	☐	☐		Investigation Team	
Review the draft investigation report							
Draft report reviewed by Lead Investigator?	22	☐	☐	☐		Lead Investigator	
Draft report provided to Person of Interest for comment?	22	☐	☐	☐		Decision Maker	
Report finalised (with consideration for POI's comments)?	22	☐	☐	☐		Investigation Team	Recommendations (if required):
Share Final Report							
Final report shared with relevant parties?	22	☐	☐	☐		Lead Investigator	Parties receiving report:
Consider disciplinary (or other) action							
Decision made based on investigation report?	22	☐	☐	☐		Decision Maker	Decision:
Matter referred to Human Resources for disciplinary (or other) action?	**2**2	☐	☐	☐		Director of Human Resources	

Stage 4: Closing the loop							
Case Name:							
Action	**Ref to Fraud Response Plan**	**Yes**	**No**	**N/A**	**Date completed**	**Completed by**	**Details / Notes / Reference / Actions**
Refer the outcome to third parties							
Outcome referred to other relevant parties?	23	☐	☐	☐		Decision Maker	Parties notified of outcome:
Update discloser							
Discloser informed of outcome (where appropriate)?	23	☐	☐	☐		Lead Investigator	
Close case file							
Investigation file up-to-date, complete and saved electronically?	23					Lead Investigator	
Communications							
Communication strategy developed (where appropriate)?	23	☐	☐	☐		Fraud Control Officer	
Internal communication appropriate or required? Media communication required?	23	☐	☐	☐		Fraud Control Officer	
	23	☐	☐	☐		Fraud Control Officer	Detail:
Recover losses							
Civil recovery options identified?	23	☐	☐	☐		Fraud Control Officer	
Asset recovery specialist?	23	☐	☐	☐		Fraud Control Officer	
Insurance?	23	☐	☐	☐		Fraud Control Officer	
Consider lessons learnt							
Incident register updated?	23	☐	☐	☐		Fraud Control Officer	
Existing gaps considered and identified?	23	☐	☐	☐		Fraud Control Officer	

Next steps identified?	23	☐	☐	☐		Fraud Control Officer	
Updates to policy/procedures needed?	23	☐	☐	☐		Fraud Control Officer	

Sign-off

Lead Investigator _____ Date: ___/___/____

Assessment Team _____ Date: ___/___/____

APPENDIX C: SUMMARY OF FRAUD PREVENTION, DETECTION AND RESPONSE ACTIVITIES AND RESPONSIBILITIES

Our Fraud and Corruption Prevention Procedures is a component of a broader integrated governance framework, policies and procedures. Its co-dependency with a number of other University policies, plans and procedures is outlined below.

Name	Action	Responsible Officer	Cycle
Ethical Behaviour Policy	Review of the Ethical Behaviour Policy	Director of Human Resources	5 years
Protected Disclosures Policy	Review of the Protected Disclosures Policy	Director of Human Resources	5 year
Conflicts of Interest Policy	Review the Conflict of Interest Policy	ORAC	5 years
Sensitive Expenditure Framework	Review the Sensitive Expenditure Policy	Financial Controller	2 years
Sensitive Expenditure Procedure and Guidelines	Review the Sensitive Expenditure Procedure and Guidelines	Financial Controller	2 years
Purchase Card Policy	Review the Purchase Card Policy	Financial Controller	5 years
Purchase Card Procedure	Review the Purchase Card Procedure	Team Leader Accounts Payable	5 years
Acceptance of Gifts, Benefits and Gratuities Policy	Review the Acceptance of Gifts, Benefits and Gratuities Policy	ORAC	5 years
Travel and Travel Related Costs Policy	Review the Travel Related Costs Framework	Director of Human Resources	5 years
Travel Planning Procedure	Review the Travel Planning Procedure	Senior Manager Procurement	2 years
Procurement Policy	Review the Procurement Policy	Senior Manager Procurement	2 years
SLT Fraud Training	Training for SLT	ORAC	One off
Fraud risk assessment	Conduct a fraud risk assessment	ORAC	3 years
Fraud risk register	Maintain and regularly report to the ARC a Fraud risk register	ORAC	Ongoing
Fraud awareness training	All line manager staff and employees in designated positions undergo fraud	ORAC	3 years

Name	Action	Responsible Officer	Cycle
	awareness training		
Fraud and Corruption general training	Fraud and Corruption training to be made available for all Staff so they understand the University's expectations on what constitutes fraud, corruption and who fraud and corruption is reported to	ORAC	Ongoing
Employee background checks	Employment screening processes	Director of Human Resources	Ongoing
Supplier vetting	All new suppliers are subject to vetting	Divisional Services and Admin	Ongoing
Payroll and On-boarding internal Audit	Determining whether controls within the payroll process exist to ensure the completeness, accuracy and validity of payroll payment. Ensuring that University Staff on-boarding process is carried out effectively and efficiently. There are controls in place to mitigate the risks identified during the review.	ORAC	3 years
Purchasing / Payables internal audit	Review of key purchases to payables processes, targeted towards higher risk areas that help ensure the integrity of purchasing master data and payment transactions. To assess if the University has processes to control who it purchases from and follows the established policies and delegations. Also to assess if there are appropriate controls over discretionary expenditure.	ORAC	3 years
Treasury Management Review	Review key controls, including delegations of authority, segregation of duties, reporting to senior management and University Council	ORAC	3 years
Travel and	Determine whether University Staff travel, and entertainment	ORAC	3 years

Name	Action	Responsible Officer	Cycle
Entertainment review	expenses are appropriate, accurate and comply with, the University's policies and procedures and Auditor General Guidelines. To ensure travel and entertainment practices across the business is consistent both at the academic and other divisions.		
Cyber Security - Penetration Testing	Complete penetration testing on the University's Information Systems	ORAC	3 years
Annual Leave Review	Compare annual leave records insurance records to identify potential un-booked annual leave.	ORAC	Annually
Suspicious Transaction Analysis/Data Mining	Perform a review of the University's transactional data using computer assisted auditing techniques	ORAC	Annually
Post transactional Review	Monthly post transactional reviews are completed over creditor's Masterfile, journals with segregation of duties risk, approval exceptions and PCards.	ORAC	Monthly
Monthly Management Reporting	University Staff reviewing the monthly Divisional reports maintain an awareness for fraud	Head of Finance Advisory	Ongoing
Cyber security prevention and detection strategies	The cyber security prevention and detection strategies are completed	Senior Manager IT Assurance & Cyber Security	Ongoing
Fraud Email address and phone	The fraud email address and phone line are monitored	ORAC	Ongoing
Insurance cover	Insurance cover is reviewed and kept up to date	Financial Controller	Ongoing
Corruption Prevention Initiatives Self-Assessment	Review the effectiveness of Fraud and Corruption Prevention initiatives (as promoted in publications such as AS8001- 2021 Fraud and	ORAC	Annual

Name	Action	Responsible Officer	Cycle
	Corruption Control, Audit Office of NSW - Fraud Control Improvement Kit Feb 2015)		
Fraud Register/Internal Reporting	Results of all fraud investigations are reported internally and registered	ORAC	As required