<INSERT ENTITY NAME> Fraud and Corruption Control System

This non-mandatory template provides the Fraud and Corruption Control Standard (AS 8001:2021) recommended structure of a fraud and corruption control system. The template summarises AS 8001:2021 minimum requirements and guidance.

Refer to MP 0105/19 *Fraud and Corruption Control Policy* for the minimum requirements with which WA health entity fraud and corruption control systems must comply.

Contents

1. Executive Summary

1.1 Introduction

***Guidance**: Introduction may include:*

- *the Fraud and Corruption Control System (FCC System) is a comprehensive framework for addressing fraud and corruption risks aimed at reducing a WA health entity's fraud and corruption exposures*
- *fraud and corruption may impact <INSERT ENTITY NAME> through:*
    - *financial loss*
    - *loss of information*
    - *penalties imposed on <INSERT ENTITY NAME> by courts and regulators*
    - *reputational impact*
    - *diversion of management energy*
    - *morale*
    - *disruption*
    - *loss of employment*
    - *financial and operational performance*
    - *ability to attract and reattain capable staff*
    - *impact on third parties, including patients and the public.*

1.2 Definition of Fraud

Fraud is defined by the Fraud and Corruption Control Standard (AS 8001:2021) as "*dishonest activity causing actual or potential gain or loss to any person or organisation including theft of moneys or other property by persons internal and/or external to the organisation and/or where deception is used at the time, immediately before or immediately following the activity*".

Fraud can take many forms, examples of situations which, in certain circumstances, may include fraud are:

- theft or obtaining property, financial advantage or any other benefit by deception
- unauthorised use of credit / purchasing card
- false timesheets, sick or annual leave claims
- providing false or misleading information, or failing to provide information where there is an obligation to do so
- causing a loss, or avoiding or creating a liability by deception
- making, using or possessing forged or falsified documents
- unlawful use of computer systems, vehicles, telephones and other property or services
- manipulating expenses or salaries

Fraud is a serious offence as prescribed by section 80A of the *Public Sector Management Act 1994*.

1.3 Definition of Corruption

Corruption is defined by AS 8001:2021 as "*dishonest activity in which a person associated with an organisation (e.g. director, executive, manager, employee or contractor) acts contrary to the interests of the organisation and abuses their position of trust in order to achieve personal advantage or advantage for another person or organisation*".

Corruption is any conduct that is improper, immoral or fraudulent and may, under certain circumstances include, but is not limited to:

- serious conflict of interest

- dishonestly using influence
- blackmail
- manipulation of procurement process
- acceptance of gifts and hospitality
- acceptance of a bribe
- misuse of information systems, internet or email
- unauthorised release of confidential, private information or intellectual property.

Corruption is a serious offence as prescribed by section 80A of the *Public Sector Management Act 1994*.

1.4 Statement of <INSERT ENTITY NAME> attitude to fraud and corruption

***Guidance**: Statement may include:*

- *fraudulent and corrupt practices within <INSERT ENTITY NAME> will not be tolerated*
- *<INSERT ENTITY NAME> is committed to establishing and maintaining an integrity environment*
- *fraud and corruption are serious risks*
- *<INSERT ENTITY NAME> is committed to controlling the risks of fraud and corruption*
- *management and staff are expected to report detected or suspected fraud or corruption in accordance with <INSERT ENTITY NAME> processes.*

1.5 Link to <INSERT ENTITY NAME>'s codes of behaviour

***Guidance**: Link to codes of behaviour may include:*

- *The WA Health Code of Conduct identifies our CORE values fundamental in all of our work and translates these values into principles that guide our conduct in the workplace. It defines the standards of ethical and professional conduct and outlines the behaviours expected of all staff within <INSERT ENTITY NAME>.*
- *Not engaging in fraudulent and corrupt behaviour is one of the Principles of Conduct with which staff must comply under the WA health system Code of Conduct.*
- *<INSERT ENTITY NAME> staff are formally required to acknowledge the WA Code of Conduct when they complete mandatory training.*

1.6 Relationship with <INSERT ENTITY NAME> other risk management plans

AS 8001:2021 minimum requirement

Entities shall ensure that fraud and corruption control initiatives are coordinated with the entity's broader risk management approach.

2. Foundations for fraud and corruption control

2.1 Roles and accountabilities

AS 8001:2021 minimum requirement

Entities shall have a FCC Sysetm which clearly defines the roles and accountabilities for controlling the entity's fraud and corruption exposures covering 2.1.1 to 2.1.6 below.

2.1.1 <INSERT ENTITY NAME> governing body

AS 8001:2021 minimum requirements

An effective FCC System requires commitment by the governing body e.g. the health service provider Board or the Director General for the Department of Health.

Entities shall implement a strategy aimed at ensuring that their governing body:

a) acknowledges and accepts overall responsibility for controlling the entity's fraud and corruption risks
b) acknowledges fraud and corruption as a serious risk
c) has an awareness of the entity's fraud and corruption exposure
d) demonstrates a high level of commitment to controlling the risks of fraud and corruption both against the entity and by the entity.

2.1.2 <INSERT ENTITY NAME> executive

AS 8001:2021 minimum requirements

An effective FCC System requires commitment by the entity's executive.

Separate to ensuring fraud and corruption control governance responsibilities are addressed by their governing body, entities shall ensure that the executive have:

a) an adequate understanding of their role in the control of the entity's fraud and corruption exposures
b) an awareness of the entity's current fraud and corruption exposures.

2.1.3 Specialist fraud and corruption control resources

AS 8001:2021 minimum requirements

Entities shall implement an appropriate level of fraud and corruption control resourcing based on the entity's assessed fraud and corruption exposures.

Entities with a person delivering a specialist fraud and corruption function shall ensure that this resource remains up-to-date with current best practice through:

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

2.1.4 Information Security Management System professionals

*Note: the appointment of an Information Security Management System (**ISMS**) professional is not a minimum requirement of AS 8001:2021. However, should an ISMS professional be appointed, the following minimum requirements apply.*

AS 8001:2021 minimum requirements

An ISMS professional, where appointed, shall have the following attributes:

a) formal qualifications appropriate to the role of an ISMS professional
b) a sound understanding of the entity's fraud and corruption exposures
c) a program for continuing professional development in technology-enabled fraud and corruption
d) a sound understanding of how an ISMS can effectively mitigate the risks of cybercrime as set out in *Information Technology – Security Techniques – Guidelines for Cybersecurity* (ISO/IEC 27032).

An ISMS professional, where appointed, shall apply principles in accordance with *Information Technology – Security Techniques – Information Security Management Systems – Requirements* (**AS ISO/IEC 27001**) in the development, implementation and maintenance of an ISMS.

2.1.5 Line management

AS 8001:2021 minimum requirements

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

Entities shall ensure that line management are fully aware that managing fraud and corruption is as much part of their responsibility as managing other types of enterprise risk.

In order to reinforce this, it is important that a system be developed and implemented with the following elements:

a) fraud and corruption control are incorporated into the performance management system
b) preventing and detecting fraud and corruption shall be specified in the position description of line managers where appropriate.

2.1.6 Other entity functions

***Guidance**: There is often a range of other internal functions within Entities that can be beneficial in the control of fraud and corruption. These internal functions will vary, but generally will include such roles as:*

a) human resources, industrial relations, payroll and learning and development
b) occupational health and safety
c) compliance professionals
d) corporate counsel
e) quality assurance
f) records management
g) insurance manager
h) regulatory affairs managers
i) environmental impact managers
j) physical security and asset management
k) procurement and accounts payable

l) finance and treasury
m) policy and program design
n) internal audit.

AS 8001:2021 minimum requirements

Entities shall ensure that fraud and corruption control initiatives are coordinated with the entity's broader risk management approach. This requires that the entity's specialist fraud and corruption control resources, including ISMS professionals (where appointed), collaborate closely with the entity's other risk management resources in order to ensure that fraud and corruption risks are incorporated into the entity's overall risk management system.

Entities shall coordinate these resources in order to control the entity's fraud and corruption exposures.

2.2 Awareness raising of fraud and corruption risk

AS 8001:2021 minimum requirements

Entities shall implement a program aimed at ensuring that the governing body, executive, specialist fraud and corruption control resources, line management and all other staff are aware of the entity's fraud and corruption exposures and how they should respond if they detect or suspect a fraud or corruption event.

Overall responsibility for ensuring that this program is implemented rests with the governing body and executive, but the day-to-day aspects shall be delegated to the specialist fraud and corruption control function or another appropriately qualified resource.

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

2.3 Business unit accountability for fraud and corruption control

AS 8001:2021 minimum requirement

Entities shall communicate to management of discrete business units, particularly business units that are geographically remote to the entity's core business functions, that they are accountable for fraud and corruption control within their business unit.

2.4 Fraud and corruption risk management

AS 8001:2021 minimum requirement

Entities shall apply the risk management principles set out in *Risk Management Guidelines* (**AS ISO 31000**) in the management of fraud and corruption risk and in doing so will apply the six stage risk management process in accordance with the AS ISO 31000 comprising of the following:

a) communication and consultation
b) scope, context and criteria
c) risk assessment
d) risk treatment
e) monitoring and review
f) recording and reporting.

2.5 External environmental scan

AS 8001:2021 minimum requirement

Entities shall systematically scan and monitor the external environment to identify fraud and corruption risks to which the entity may be exposed.

2.6 Developing and implementing an FCC System

AS 8001:2021 minimum requirements

Entities shall develop and implement a FCC System incorporating the entity's approach to controlling fraud and corruption exposures at strategic, tactical and operational levels

In preparing and implementing such a system, entities shall analyse the following:

a) contextual factors including the entity's size, composition, head count, geographic footprint and risk profile
b) industries in which the entity operates
c) economies, markets and jurisdictions in which the entity operated with particular regard to applicable laws and regulations.

The FCC System shall seek to control:

i) internal fraud and corruption against the entity and its operations
ii) external fraud and corruption against the entity and its operations
iii) fraud and corruption involving persons internal to the entity in collaboration with persons external to the entity
iv) fraud and corruption by the entity or by persons purporting to act on behalf of and in the interest of the entity.

The FCC System shall include the entity's intended action in implementing and monitoring the entity's fraud and corruption prevention, detection and response initiatives.

The FCC System shall take into account any existing policies and procedures relevant to fraud and corruption risk.

Entities shall document the FCC System.

Entities shall effectively communicate and promote the FCC System internally within the entity and, where appropriate, externally to the entity.

A program for monitoring the implementation, operation and maintenance of the FCC System shall be established, including key milestones and resourcing requirements.

The FCC System shall be reviewed at least biennially and amended as appropriate.

2.7 Leveraging the internal audit function in fraud and corruption control

AS 8001:2021 minimum requirement

As fraud poses a serious threat to an entity's value (both in financial and reputational terms) it is essential that an entity's internal audit function (where such a function exists) is alert to and considers the entity's fraud exposures with the objective of providing objective assurance as to the effectiveness of controls in mitigating, detecting and reporting fraud events.

2.8 Leveraging the external audit function in fraud and corruption control

AS 8001:2021 minimum requirements

Governing bodies and executive of entities whose financial statements are audited shall be informed as to the role and responsibilities of the auditor in detecting fraud.

The governing body and/or audit committee of an audited entity shall 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 entity's financial statements due to fraud. Audited entities shall take a proactive position in relation to the audit fraud detection program including:

a) informing the auditor of the entity's fraud and corruption detection philosophy and the importance the entity places on fraud detection as part of the audit
b) aiding the auditor to enable a more comprehensive examination of fraud and corruption issues
c) an internal consideration of fraud risk factors as defined in *The Auditor's Responsibilities Relating to Fraud in an Audit of a Financial Report Issued by the Auditing and Assurance Standards Board* (ASA 240).

2.9 Implementing an Information Security Management System

AS 8001:2021 minimum requirements

Entities shall implement an ISMS in accordance with AS ISO/IEC 27001, incorporating the following elements:

a) context of the entity
b) leadership
c) planning
d) support
e) operation
f) performance evaluation
g) improvement.

2.10 Record keeping and confidentiality of information

AS 8001:2021 minimum requirements

Entities shall have policies, procedures and systems that require staff to maintain accurate and complete records of business activity. Record keeping requirements are derived from an entity's broad operating context including the entities:

a) business needs
b) legal and regulatory requirements
c) community and societal expectations.

An entity's policies, procedures and systems shall also:

i) set out mechanisms for identifying and protecting information that is confidential
ii) establish criteria for monitoring compliance and taking any necessary corrective action
iii) regard any deliberate failure to maintain complete and accurate records as a disciplinary matter.

2.11 Consideration of extra-jurisdiction implications

Note: the clause "Consideration of extra-jurisdiction implications" was included in the draft AS 8001:2020, but is not included in AS 8001:2021. The guidance provided by draft AS 8001:2020 is included below.

***Guidance**: In the increasingly globalised economy, many organisations operate across multiple jurisdictions. This leads to a number of consequences for the prevention, detection and response of an organisation's fraud and corruption exposures and events. Organisations operating externally to the Australian economy should investigate how fraud and corruption exposures will be impacted by its ex-jurisdictional operations and specifically:*

a) local legislation that impacts the organisation's fraud and corruption initiatives
b) cultural norms relative to Australian cultural norms
c) the need to comply with relevant Australian legislation in relation to foreign operations.

3. Fraud and corruption prevention

AS 8001:2021 minimum requirement

The initiatives that entities shall put in place in the context of proactive prevention of fraud and corruption are 3.1 to 3.9 below.

3.1 Promoting a sound integrity framework

AS 8001:2021 minimum requirements

An integrity framework shall be developed using a participatory approach aimed at building commitment within the entity's workforce and other interested parties. Such a framework shall include a process for benchmarking and continuous monitoring of the entity's integrity environment underpinned by example setting by the entity's governing body and executive.

An entity's integrity framework shall include the policy and structural elements as set out in Table 1.

Table 1: Fundamental elements of an integrity framework

Element		Description
1	Example setting	Observable adherence to the entity's integrity framework by the governing body and executive.
2	Governing body commitment	Statement of commitment by the entity's governing body to establish and maintain an integrity environment and to actively promote such a culture.
3	Codes of behaviour	A Code of Ethics or Code of Conduct incorporating high-level aspirational statement of values with examples of conduct the entity deems unacceptable.
4	Allocation of responsibility	Responsibility assigned to a senior person for ensuring the entity's integrity initiatives are implemented and monitored. The person would have a direct line of reporting to an ethics committee or other committee with overall responsibility for the entity's integrity environment. In addition to allocation of specific responsibility for improving the entity's performance on this issue, it should be clearly communicated internally that every person associated with the entity has a role to play in driving positive integrity and ethical behaviours.
5	Ethics committee	An ethics committee, once appointed, is the body charged with overseeing the operation and maintenance of the entity's entire integrity framework. It can also be the final arbiter on issues of apparent misconduct and integrity dilemmas that cannot otherwise be resolved at line-management level. This committee can either be a board or management committee as appropriate to the entity's governance framework.
6	Risk-based approach	Implementation of Integrity Framework (including prevention of fraud and corruption) is to be done through the application of risk management practices and risk-based approach (outlined in AS ISO 31000)

3.2 Managing conflicts of interest

AS 8001:2021 minimum requirements

Entities shall take the following actions:

a) have a policy and/or procedure that requires staff, volunteers, students on placement and relevant business associates to disclose actual, potential or perceived conflicts of interest. This policy and/or procedure may form part of the code of behaviour or be a stand-alone document
b) maintain records of relevant business, financial, family, political or personal interests of staff that could conflict with their entity-wide duties
c) maintain records of actions taken to avoid, eliminate or manage any perceived, potential and/or actual conflicts of interest identified
d) require management to monitor and actively manage risks posed by conflicts of interest
e) include information about conflicts of interest in relevant training programs
f) seek to identify concealed conflicts of interest as part of the entity's fraud and corruption detection program
g) treat a failure to disclose or properly manage a conflict of interest as a potential disciplinary matter or a breach of contract.

3.3 Managing risks connected to gifts, hospitality, donations and similar benefits

AS 8001:2021 minimum requirements

Gifts, hospitality, donations and similar benefits may be aimed at or perceived by a third party as being aimed to influence a person. To manage this corruption risk, entities shall:

a) document a policy on gifts, hospitality, donations and similar benefits
b) maintain record of and monitor gifts, hospitality, donations and similar benefits
c) maintain records of actions taken if breach of the gifts, hospitality, donations and similar benefits policy has occurred
d) include information about managing gifts, hospitality, donations and similar benefits in relevant training programs
e) annual review compliance with the policy.

3.4 Implementing and maintaining an internal control system

AS 8001:2021 minimum requirements

Entities shall ensure that all business processes are subject to a system of internal control that is well documented, regularly updated and understood by all staff involved with these processes.

Entities shall implement the following aspects of an internal control system as part of the entity's FCC System:

a) internal controls that are, to an appropriate degree, risk focused, i.e. they have been developed after the entity has identified and assessed the risks it faces and are aimed at mitigating those risks. This shall involve development of internal controls that target risks identified by application of AS ISO 31000
b) internal controls that are appropriately documented
c) a process of continuous improvement. Internal controls that are reviewed and amended regularly

d) internal controls that are communicated effectively to all staff appropriate to their level of responsibility and position description
e) internal controls that are accessible to personnel. If an entity's personnel have ready access to the entity's intranet site, the most recent version of a given internal control system can be quickly and effectively accessed
f) a strong internal control culture in which all personnel understand the importance of adhering to internal control. This may include internal control adherence as an element of the regular performance review program
g) a program for assessing compliance with the entity's internal controls. This can be done by way of an online staff survey or compliance audits
h) the entity's governing body and executive setting an example of internal control adherence
i) an internal audit program that incorporates a review of adherence to internal control.

Entities shall implement procedures aimed as assessing the operating effectiveness of internal controls. These procedures are often referred to as "pressure testing".

A pressure testing program shall be carefully designed to ensure there is no financial or non-financial loss to the entity.

The entity shall ensure that weak or failed internal controls identified by the pressure testing program are remediated.

Entities conducting pressure testing shall have the following governance arrangements in place:

A. appropriate accountability arrangements for senior executives and officers involved in pressure tests
B. record keeping for key decisions, recommendations and actions
C. processes for choosing pressure tests, e.g. fraud or corruption risks with high risk ratings or high reliance on manual controls
D. processes for sharing results and collaborating with relevant internal and external interested parties.

3.5 Incentives and performance indicators

AS 8001:2021 minimum requirement

Entities shall consider performance targets as part of the risk assessment process set out in 2.4.

3.6 Workforce screening

AS 8001:2021 minimum requirements

Entities shall conduct workforce screening in accordance with *Employment Screening* (AS 4811).

Entities shall develop a process that provides for effective workforce screening of entrusted persons:

a) before appointment
b) upon promotion or change of employment circumstances particularly if the person is being promoted to a senior position or a position involving higher risk of fraud or corruption
c) prior to the completion of the probationary period.

3.7 Screening and ongoing management of business associates

AS 8001:2021 minimum requirements

Entities shall ensure the integrity of new business associates and periodically confirm the bona fides of ongoing business associates.

Entities shall develop procedures that provide for effective vetting of business associates.

Where an entity's fraud and corruption risk assessment has assessed a significant corruption risk exposure in relation to:

a) specific categories of transactions, projects or activities
b) planned or ongoing relationships with specific categories of business associates
c) specific categories of staff in certain positions

the entity shall assess the nature and extent of the fraud and corruption risk in relation to specific transactions, projects, activities, business associates and staff falling within those categories. This assessment shall include due diligence necessary to obtain sufficient information to assess the fraud and corruption risk. The due diligence assessment shall be updated at a defined frequency, so that changes and new information can be properly considered.

Entities shall, on the basis of their due diligence activities, require business associates to adopt a FCC System that conforms to AS 8001:2021 or specified aspects of it.

3.8 Preventing "technology-enabled" fraud

AS 8001:2021 minimum requirements

In light of the increased fraud risks associated with information technologies, entities shall continuously assess their exposure to technology-enabled fraud, aimed at better informing themselves as to the fraud risks relevant to their operations and therefore their prevention and detection requirements.

Entities shall implement an information security management framework or system.

3.9 Physical security and asset management

AS 8001:2021 minimum requirement

Entities shall risk assess their physical security environment in order that appropriate measures are put in place to prevent the theft of valuable tangible assets.

4. Detecting fraud and corruption

AS 8001:2021 minimum requirements

An entity's FCC System shall incorporate fraud and corruption detection actions covering 4.1 to 4.9 below, in the proactive detection of fraud and corruption against or by the entity, based on their assessed exposure to fraud and corruption.

4.1 Post-transactional review

AS 8001:2021 minimum requirement

Entities shall implement a program for detection of fraud and corruption events by post-transactional review that is appropriate for the entity's assessed fraud and corruption exposures.

4.2 Analysis of management accounting reports

AS 8001:2021 minimum requirement

Entities shall implement a program for detection of fraud and corruption events by analysis of management accounting reports that is appropriate for the entity's assessed fraud and corruption exposures.

4.3 Identification of early warning signs

AS 8001:2021 minimum requirement

Entities shall implement a program for detection of fraud and corruption events by identification of early warning signs that is appropriate for the entity's assessed fraud and corruption exposures.

4.4 Data analytics

AS 8001:2021 minimum requirement

Entities shall apply data analytic techniques in the detection of fraud and corruption. In doing so, entities shall design data analytic tests that capture relevant indicators of the entity's fraud or corruption exposures.

4.5 Fraud and corruption reporting channels

AS 8001:2021 minimum requirements

Entities shall implement a program for detection of fraud and corruption events establishing a range of fraud and corruption reporting channels.

Entities shall encourage staff and other interested parties who have concerns or suspicions of fraudulent or corrupt conduct to come forward and promptly report them.

Entities shall also ensure that adequate means for reporting suspicious or known illegal or unethical conduct are available to all staff and interested parties.

Both internal and externally operated alternative reporting lines shall allow anonymous reporting.

4.6 Public Interest Disclosures

AS 8001:2021 minimum requirements

Entities shall implement a system for the protection and active support of individuals connected with the entity who report or who wish to report suspected cases of fraud or corruption in addition to other types of wrongdoing.

Entities shall implement an appropriate Public Interest Disclosure (**PID**) management system taking in account relevant guidance provided by the *Public Interest Disclosure Act 2003*.

The entity's PID management system shall be documented in a policy that includes the following:

a) a strong statement of purpose
b) a clear statement of governing body commitment to the PID management system
c) linkage to the values of the entity and the entity's code of behaviour
d) a statement as to the classes of people who will be considered to be making a PID
e) a clear statement about the types of wrongdoing to which the policy applies
f) a clear statement about how a discloser can make a PID
g) a clear statement requiring the entity to protect the identity of the discloser in the event that the discloser wishes to remain anonymous
h) the appointment of a discloser protection officer (a separate function to the function that is responsible for investigating PIDs) or similar whose role will be to protect the discloser
i) details as to how the discloser protection officer will actively protect disclosers
j) a clear statement that all information provided by a discloser is held in the strictest confidence unless disclosure has been authorised by the discloser or disclosure is required by law
k) a requirement to provide feedback to disclosers
l) a clear statement banning detrimental conduct against a discloser who has come forward as well as any person who is considering coming forward or who the person engaging in detrimental conduct believes may in the future come forward
m) information about how the entity will investigate disclosures that qualify for protection
n) information about how the entity will ensure fair treatment of staff who are mentioned in disclosures that qualify for protection under the PID policy, or to whom such disclosures related
o) a program for training and promotion
p) monitoring the performance and effectiveness of the PID management system
q) information about how the policy is to be made available to officers and staff of the entity
r) details about how the policy will be reviewed and the frequency of reviews
s) resourcing a PID management function with responsibility for the system and appropriate authority
t) the entity's position with regard to compensating disclosers who are subject to reprisal by an individual or by the entity itself
u) the entity's position with regard to rewarding disclosers for reporting conduct to which the policy relates.

4.7 Leveraging business associates and other external parties

***Guidance**: Statements of business integrity, contracts or other arrangements with business associates and third parties should:*

a) clearly state the entity's expectation that business associates and third parties act ethically
b) outline the internal and external reporting channels for business associates and third parties to report suspicions of fraud and corruption that involves or may have an impact on the entity

c) assure business associates and third parties that they will not face detriment for reporting their concerns.

4.8 Complaint management

AS 8001:2021 minimum requirements

Entities shall establish a system for handling complaints in line with *Guidelines for Complaint Management in Organisations* (AS/NZS 10002).

Frontline and communications staff shall be trained in recognising and escalating complaints about fraud and corruption.

4.9 Exit interview

AS 8001:2021 minimum requirement

Entities shall adopt a program of exit interviews for all terminated staff.

5. Responding to fraud and corruption events

AS 8001:2021 minimum requirement

Entities shall incorporate their programmed response to fraud and corruption events in a response and recovery plan which will clearly set out the entity's response to detected fraud and corruption events. The response and recovery plan forms part of the FCC System.

5.1 Immediate action on discovery of a fraud or corruption event

AS 8001:2021 minimum requirements

Entities shall develop a procedure for immediate action in response to a fraud and corruption event.

Immediate action taken in response to the discovery of a fraud or corruption event shall be documented, including how the event was identified and the considerations, actions and assessments taken.

Entities shall develop a procedure for first response of the capture of digital evidence in relation to a detected or suspected fraud or corruption event in accordance with *Information Technology – Security Techniques – Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence* (**ISO/IEC 27037**).

Entities shall ensure that digital evidence first responders responding to a fraud and corruption event involving digital evidence are qualified to do so (in accordance with ISO/IEC 27037) and comply with the entity's own first response procedure in accordance with ISO/IEC 27037.

5.2 Investigation of a detected fraud or corruption event

AS 8001:2021 minimum requirements

An investigation into apparent or suspected fraud and corruption shall be conducted by appropriately skilled and experienced investigators who are independent of the business unit in which the alleged fraudulent or corrupt conduct occurred.

Investigations of fraud and corruption events shall be conducted in accordance with the following principles:

a) external parties engaged to assist in investigations on an entity's behalf shall enter into a binding agreement in relation to the release of confidential information coming into their possession during the course of the investigation
b) any investigation and resulting disciplinary proceedings shall be conducted in an atmosphere of transparency ensuring that the rules of natural justice are observed
c) the overall guiding principles of any investigation into alleged improper conduct shall be independence and objectivity
d) adequate records shall be prepared and maintained for all investigations
e) an entity investigating allegations of fraud or corruption shall ensure that information arising from, or relevant to, the investigation is only disseminated to anyone who has a defined role in the investigation or the resolution of matters under investigation
f) any investigation into a fraud or corruption event within an entity shall be subject to an appropriate level of supervision by an independent person or committee within the entity having regard to the seriousness of the matter under investigation. In serious cases, the investigation shall be monitored by the audit committee, the ethics committee or the governing body.

When assessing and investigating allegations, entities shall direct their attention primarily to the available evidence rather than the perceived motives of the reporter.

Investigation planning

AS 8001:2021 minimum requirements

Any investigation shall be adequately planned. Such an investigation plan shall document the following:

a) background to the matter
b) objectives of an investigation
c) preliminary steps to be taken before commencement of the substantive phases of the investigation
d) resourcing (internal and external)
e) potential sources of evidence
f) dealing with witnesses
g) dealing with PIDs (including discloser protection and support)
h) legal considerations in terms of capturing evidence
i) analysis of evidence captured
j) storage of evidence (digital and non-digital) including ensuring that the chain of custody can be proven
k) risks associated with the investigation
l) risk of harm to investigators
m) notification, at an appropriate time, of persons suspected of involvement in illegal or improper conduct that an investigation is being conducted
n) reporting.

Investigators

AS 8001:2021 minimum requirements

Entities shall ensure that investigators have the relevant skills, qualifications or training to effectively carry out the investigation.

Entities shall assess and manage the ongoing suitability of investigators tasked with investigating a fraud or corruption event.

An entity shall risk assess and have appropriate protocols and training in place to ensure the safety of all investigators tasked with conducting investigations.

Evidence

AS 8001:2021 minimum requirements

Entities shall develop an entity-specific procedure for capturing digital evidence in relation to a detected or suspected fraud or corruption event in accordance with:

- ISO/IEC 27037
- *Information Technology – Security Techniques – Guidance on Assuring Stability and Adequacy of Event Investigative Method* (ISO/IEC 27041)
- *Information Technology – Security Techniques – Guidelines for Analysis and Interpretation of Digital Evidence* (ISO/IEC 27042)
- *Information Technology -Security Techniques – Incident Investigation Principles and Processes* (ISO/IEC 27043)

- *Computer Security Incident Handling Guide* (NIST SP 800-61 Rev. 2).

Entities shall ensure that all staff undertaking the capture, analysis and management of digital evidence in the context of fraud and corruption investigation (staff internal to the entity as well as external resources) are trained in accordance with the ISO/IEC and NIST standards above.

All evidence (other than digital evidence) captured shall be:

i) adequately recorded at the time it is captured
ii) held securely at all times
iii) adequately accounted for each time it is handed from one party to another party (chain of custody).

Record keeping

AS 8001:2021 minimum requirements

Entities shall maintain complete, accurate records of all investigations conducted into a fraud or corruption event.

Because investigations often involve a covert phase and require the collection of material that is private, sensitive or controversial, records shall only be accessible to staff with an identified "need-to-know".

In relation to evidence, entities shall record the following:

a) the source of all evidence and exhibits and the associated continuity of custody, including the return or destruction of evidence
b) oral evidence by making an electronic audio/video recording (with the knowledge of the participant) and/or by converting it into written form (preferably signed or acknowledged as true and accurate by the participant).
c) all exculpatory evidence.

In relation to case management, entities shall record the following:

i) an itemised list of the allegations under investigation
ii) the investigation system
iii) key decisions, actions and communications
iv) working papers that demonstrate the investigative procedures performed and the basis for findings and conclusions
v) details of liaison with law enforcement and regulatory authorities
vi) proof of adherence to principles of procedural fairness
vii) any documents or things that are the subject of legal professional privilege
viii) the use of any investigative powers and the source of those powers (e.g. statute, contract, industrial award, policy).
ix) the investigation report and all attachments
x) quality review of the investigation and investigation report.

5.3 Disciplinary procedures

AS 8001:2021 minimum requirements

Entities shall ensure that their own Human Resources Manual (or other relevant internal policies or guidelines) includes particulars on how disciplinary proceedings should be conducted.

To separate the investigation and determination process in relation to the investigation of a fraud or corruption event, the entity shall have a process for ensuring the findings of an investigation into a fraud or corruption event are referred by the investigation function to an independent person or committee.

5.4 Crisis management following discovery of a fraud or corruption event

***Guidance**: Entities should have a crisis management system for dealing with fraud or corruption events. The crisis management system should include procedures to follow and the approach to be taken when a suspected case of fraud or corruption has been detected especially is senior staff are implicated.*

5.5 Internal reporting and escalation

AS 8001:2021 minimum requirements

Entities shall develop and implement a system for the capturing, reporting, analysis and escalation of all detected fraud and corruption events.

Entities shall establish a fraud and corruption event register and shall ensure that all fraud and corruption events occurring (subject to minimum reporting thresholds) are entered therein.

The fraud and corruption event register shall be maintained by the entity's specialist fraud and corruption control resource (where appointed) or other responsible person.

Entities shall implement a program for the centralised capture of all fraud and corruption events and ensure that this data are used in the effective measurement of fraud and corruption against or by the entity.

5.6 External reporting

AS 8001:2021 minimum requirements

Entities shall have a policy on whether and how allegations of fraudulent and corrupt conduct are reported to the police, other appropriate law enforcement agency, or other government body (for example, as identified in legislation).

Any relevant obligations shall form part of the entity's external reporting policy.

The entity's external reporting policy shall be consistently applied so that there can be no suggestion of selective application.

In the event that a decision is made to refer the matter to the appropriate law enforcement agency the entity shall give an undertaking to the law enforcement agency that it will do all that is reasonable in assisting the agency to conduct a full and proper investigation.

5.7 Recovery of stolen funds or property

AS 8001:2021 minimum requirement

Entities shall have a policy requiring consideration of legal action for recovery of stolen funds or property where there is evidence of fraud or corruption and where the benefits of such recovery are considered worthwhile.

5.8 Responding to fraud and corruption events involving business associates

AS 8001:2021 minimum requirement

Where an entity finds evidence of fraud or corruption by a business associate (including contractors and subcontractors), the entity shall take proportionate action.

5.9 Insuring against fraud events

AS 8001:2021 minimum requirement

Entities shall undertake a risk assessment as to whether it is appropriate to hold relevant insurance that indemnifies the entity against the risk of loss arising from fraudulent conduct.

5.10 Assessing internal controls, system and processes post detection of a fraud or corruption event

AS 8001:2021 minimum requirements

In each instance where a fraud or corruption event is detected, the specialist fraud and corruption control function (if appointed) and relevant line management shall reassess the adequacy of the internal control environment, particularly those controls directly impacting on the fraud or corruption event and potentially allowing it to occur, and consider whether remediation or enhancements to existing controls are required.

Such a review shall address the following:

a) assessing the adequacy of the internal control environment and consideration of whether improvements are required
b) recommendations aimed at improved mitigation of fraud and corruption risks.

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

Relevant findings from an investigation report shall be conveyed to the process and risk owners to allow risks to be re-evaluated and treated.

Responsibility for monitoring internal control remediation following an investigation into a fraud or corruption event shall be allocated to an individual with significant authority (e.g. the specialist fraud and corruption control function).

All remedial action proposed in response to a fraud or corruption event shall be reported to the entity's audit and risk committee or similar oversight body which shall be responsible for ensuring that all remedial action in relation to internal controls has been effected.

Entities shall also periodically analyse the body of investigation reported in order to identify relevant trends, patterns or areas for internal control improvement.

5.11 Third parties

***Guidance**: Entities should consider the impact of a fraud or corruption event on third parties including the following:*

a) customers and clients
b) government services, including law enforcement, prosecutors, courts, tribunals and legal aid
c) community
d) environment
e) industry
f) security.

5.12 Disruption of fraud and corruption

AS 8001:2021 minimum requirement

Entities shall include the concept of “disruption” as part of their suite of potential responses to fraud and corruption events.

Glossary

Term Used	Definition
AS 8001:2021	Fraud and corruption control Standard
Bona fides	Evidence showing that a person or organisation's business practices are straightforward and of integrity.
Bribe	A gift or benefit offered or solicited by a staff member to influence that person to act in a particular way and to induce the staff member to act in a way that is contrary to the known rules of honesty and integrity.
Business associate	External party with who <<INSERT ENTITY NAME>> has, or plans to establish, some form of business relationship. A business associate includes, but is not limited to: • contractors • consultants • participants in work experience • persons delivering training or education • public private partnerships • recruitment agencies • researchers • sub-contractors • suppliers • universities and TAFE colleges.
Conflict of interest	A situation arising from conflict between the performance of public duty and private or personal interests. Conflicts of interest may be actual, or be perceived to exist, or potentially exist at some time in the future.
Corruption	Corruption is defined by Australian Standard AS 8001:2021 as: "*Dishonest activity in which a person associated with an organisation (e.g. director, executive, manager, employee or contractor) acts contrary to the interests of the organisation and abuses their position of trust in order to achieve personal advantage or advantage for another person or organisation*". Corruption is any conduct that is improper, immoral or fraudulent and may, under certain circumstances include but is not limited to: • serious conflict of interest • dishonestly using influence • manipulation of procurement process • acceptance of gifts and hospitality • acceptance of a bribe • misuse of information systems, internet or email • unauthorised release of confidential, private information or intellectual property.

Term Used	Definition
	Corruption is a serious offence as prescribed by s. 80A of the *Public Sector Management Act 1994*.
Fraud	Fraud is defined by Australian Standard AS 8001:2021 as "*dishonest activity causing actual or potential gain or loss to any person or organisation including theft of moneys or other property by persons internal and/or external to the organisation and/or where deception is used at the time, immediately before or immediately following the activity*". Fraud can take many forms, examples of situations which, in certain circumstances, may include fraud are: • theft or obtaining property, financial advantage or any other benefit by deception • unauthorised use of credit / purchasing card • false timesheets, sick or annual leave claims • providing false or misleading information, or failing to provide information where there is an obligation to do so • causing a loss, or avoiding or creating a liability by deception • making, using or possessing forged or falsified documents • unlawful use of computer systems, vehicles, telephones and other property or services • manipulating expenses or salaries. Fraud is a serious offence as prescribed by s. 80A of the *Public Sector Management Act 1994*.
Fraud and Corruption Control System	A framework for controlling the risks of fraud and corruption against or by an organisation.
Information Security Management System	A set of interrelated and interacting elements that establishes, implements, operates, monitors, reviews, maintains and improves information security.
Information Security Management System professional	Person who establishes, implements, maintains and continuously improves one or more information security management system processes.
Integrity	The expected standards of behaviour and actions of staff which reflect honesty, accountability, transparency, impartiality, and acting with care and diligence.
Interested parties	A person or organisation that can affect, be affected by, or perceive itself to be affected by a decision or activity.
Investigation	A systematic process to discover the facts/particulars relating to the complaint/incident that may concern a breach of discipline and leads to the examination and analysis of the evidence. All investigations must result in or lead to an outcome.

Term Used	Definition
Pressure testing	Procedures aimed as assessing the operating effectiveness of internal controls.
Public Interest Disclosure	An appropriate disclosure of public interest information to a proper authority.
Serious offence	Has the same meaning as section 80A of the *Public Sector Management Act 1994.* Serious Offence means: (a) an indictable offence against a law of the State (whether or not the offence is or may be dealt with summarily), another State or a Territory of the Commonwealth or the Commonwealth (b) an offence against the law of another State or a Territory of the Commonwealth that would be an indictable offence against a law of this State if committed in this State (whether or not the offence could be dealt with summarily if committed in this jurisdiction) (c) an offence against the law of a foreign country that would be an indictable offence against a law of the Commonwealth or this State if committed in this State (whether or not the offence could be dealt with summarily if committed in this jurisdiction) (d) an offence, or an offence of a class, prescribed under section 108 (see Offences Prescribed).
Technology-enabled fraud	Fraud against or by an entity which relies heavily on information technologies and which would not be possible without information technologies.
WA health entities	WA health entities include: (i) health service providers as established by an order made under section 32 (1)(b) of the *Health Services Act 2016*. (ii) Department of Health as an administrative division of the State of Western Australia pursuant to section 35 of the *Public Sector Management Act 1994*.

This document can be made available in alternative formats on request for a person with disability.