

OFFICIAL



Australian Government

Comcare

# FRAUD CONTROL POLICY

OFFICIAL

CONTENTS

INTRODUCTION	3
Purpose	3
Scope	3
Principles	3
POLICY STATEMENT	4
SUPPORTING INFORMATION	5
Definitions	5
Related legislation, procedures, and guidelines	5
Related training	6
Change history	6
APPROVAL AND REVIEW DETAILS	6

# INTRODUCTION

## Purpose

1. Section 10 of the Public Governance, Performance and Accountability Rule 2014 (Fraud Rule) requires that the Accountable Authority of a Commonwealth entity must take all reasonable measures to prevent, detect and deal with fraud relating to the entity. Accountability and responsibility for Comcare's fraud control policy and plan lies with the CEO (as the 'accountable authority').
2. The purpose of this policy is to confirm and communicate Comcare's commitment to prevent, detect and respond to internal and external fraud and corruption.

## Scope

3. This policy applies to all Comcare officials including all ongoing and non-ongoing employees and contractors.

## Principles

4. This policy is underpinned by the following principles:
  - a. We are committed to meeting public expectations of integrity, accountability, independence, transparency and professionalism.
  - b. We require Comcare officials to act in accordance with the APS Code of Conduct and Comcare's values to prevent, detect and deal with fraud and corruption against Comcare.
  - c. Comcare will follow Commonwealth fraud guidance and fraud policy as good practice in meeting the requirements of the fraud rule<sup>1</sup>.

---

<sup>1</sup> Comcare must comply with the fraud rule. While not bound by the Commonwealth Fraud Control Policy or Commonwealth fraud guidance, both documents are good practice for corporate Commonwealth entities.

## POLICY STATEMENT

5. Comcare is committed to the prevention, detection and investigation of all fraudulent and corrupt activities. Comcare does not tolerate fraudulent or corrupt practices by officials, contractors or external parties including claimants, service providers, and those agencies and entities that Comcare regulates.
6. Comcare recognises that fraud and corruption against Comcare can:
  - a. compromise the integrity of the workers' compensation scheme
  - b. impact Comcare's regulatory activities
  - c. cause financial damage to Comcare
  - d. negatively affect Comcare's officials, operations, systems and services
  - e. compromise the reputation of Comcare, its clients and stakeholders
  - f. harm the morale of Comcare officials.
7. All officials are required to:
  - a. perform their duties with professionalism, honesty and integrity in accordance with the APS Code of Conduct and Comcare's values
  - b. comply with Comcare policies and procedures including the Fraud Control Plan,
  - c. complete annual Fraud Awareness and APS Values and Principles training
  - d. report suspected instances of fraud or corruption.
8. Comcare is committed to reducing its fraud and corruption risk profile through:
  - a. a Fraud Control Plan
  - b. maintaining fraud and corruption risk assessments (Enterprise and Group level)
  - c. delivery of training to Comcare officials and awareness in ethics, privacy, fraud and corruption
  - d. requiring professional and ethical conduct by Comcare officials
  - e. activities to prevent, detect and respond to fraud and corruption
  - f. investigating allegations of fraud and corruption, or referring matters to the appropriate law enforcement body
  - g. applying appropriate criminal, civil, administrative or disciplinary action, and
  - h. reporting incidents of fraud and corruption to the Commonwealth Government in a transparent and accountable manner.



## SUPPORTING INFORMATION

### Definitions

Term/ Phrase	Definition
<b>Comcare officials</b>	Comcare employees and contractors
<b>Corruption</b>	The dishonest or biased exercise of Commonwealth public official functions.
<b>Fraud</b>	Dishonestly obtaining a benefit, or causing a loss, by deception or other means.
<b>Fraud Guidance</b>	Attorney-General's Department's Resource Management Guide No. 201 – Preventing, Detecting and Dealing with Fraud
<b>Fraud Policy</b>	Commonwealth Fraud Control Policy
<b>Fraud Rule</b>	Section 10 of the Public Governance, Performance and Accountability Rule 2014
<b>PGPA Act</b>	<i>Public Governance, Performance and Accountability Act 2013</i>

### Related legislation, procedures, and guidelines

Document name	Link
Public Governance, Performance and Accountability Rule 2014	<a href="#"><i>Public Governance, Performance and Accountability Rule 2014</i></a>
<i>Crimes Act 1914</i>	<a href="#"><i>Crimes Act 1914</i></a>
<i>Criminal Code Act 1995</i>	<a href="#"><i>Criminal Code Act 1995</i></a>
<i>Public Interest Disclosure Act 2013 (PID Act)</i>	<a href="#"><i>Public Interest Disclosure Act 2013</i></a>
The Fraud Rule (section 10 of the Public Governance, Performance and Accountability Rule 2014)	<a href="#"><i>Section 10 – Preventing, detecting and dealing with fraud.</i></a>
Commonwealth Fraud Control Framework including the Resource Management Guide No. 201, Preventing, detecting and dealing with fraud	<a href="#"><i>Commonwealth Fraud Control Framework</i></a>
Australian Government Investigation Standards	<a href="#"><i>Australian Government Investigation Standards</i></a>
Australian Public Service Code of Conduct	<a href="#"><i>APS Values and Code of Conduct</i></a>
Commonwealth Risk Management Policy	<a href="#"><i>Commonwealth Risk Management Policy</i></a>
Accountable Authority Instructions 1 – Corporate Governance	<a href="#"><i>Accountable Authority Instructions 1 – Corporate Governance</i></a>
Comcare Compliance and Enforcement Policy	<a href="#"><i>Comcare Compliance and Enforcement Policy</i></a>
Comcare Risk Management Policy	<a href="#"><i>Comcare Risk Management Policy</i></a>
Comcare Assurance Policy	<a href="#"><i>Comcare Assurance Policy</i></a>
Comcare Fraud and Corruption Control Plan	<a href="#"><i>Fraud and Corruption Control Plan</i></a>
Public Interest Disclosures	<a href="#"><i>Public Interest Disclosures</i></a>
Comcare Code of Conduct Procedure	<a href="#"><i>Code of Conduct Procedure</i></a>

## Related training

Document name	Link
Corporate Fundamentals: Fraud Awareness	<i>Via ComLearn</i> <u><a href="#">Corporate Fundamentals: Fraud Awareness</a></u>
Corporate Fundamentals: APS Values and Principles	<i>Via ComLearn</i> <u><a href="#">Corporate Fundamentals: APS Values and Principles</a></u>

## Change history

Version	Date	Author	Reason for change
0.1	28 September 2021	s 47F	Review and update to align with Governance Framework

## Approval and review details

Document Reference	DOC6057694
Document Version Number	0.1
Policy Owner	Chief Operating Officer
Responsible Business Area	Finance and Assurance
Superseded Policies	Fraud Control Policy and Plan 2020 -2022, 21 July 2020
Approved By	Executive Committee
Date Approved	28 September 2021
Date Effective	28 September 2021
Next Review Date	30 June 2024

OFFICIAL



Australian Government

Comcare

# FRAUD CONTROL PLAN

2021–2023

OFFICIAL

# CONTENTS

<b>INTRODUCTION</b>	<b>3</b>
Purpose	3
Scope	3
Principles	3
<b>DEFINITION OF FRAUD AND CORRUPTION</b>	<b>4</b>
Fraud	4
Corruption	4
<b>LEGISLATION AND COMMONWEALTH FRAUD CONTROL FRAMEWORK</b>	<b>5</b>
<b>FRAUD AND CORRUPTION CONTROL FRAMEWORK</b>	<b>5</b>
Strategies	5
Prevention	5
Detection	6
Response	6
Risk assessments	6
Fraud risk appetite	6
Culture and values	7
<b>REPORTING FRAUD AND CORRUPTION</b>	<b>7</b>
Reporting by Comcare officials	7
Reporting by external stakeholders	7
<b>MONITORING AND REPORTING</b>	<b>8</b>
<b>SUPPORTING INFORMATION</b>	<b>8</b>
Definitions	8
Roles and responsibilities	9
Related legislation, procedures, and guidelines	10
Related training	10
Change history	10
Approval and review details	11

# INTRODUCTION

## Purpose

1. Fraud against the Commonwealth is a significant matter for all Australian Commonwealth entities and the Australian public, preventing taxpayer dollars from reaching intended targets and impacting the delivery of key services.
2. The Comcare Fraud Control Plan 2021-23 (the Plan) represents Comcare's commitment to prevent, detect and respond to internal and external fraud and corruption. The Plan outlines Comcare's approach to the management of fraud and corruption risks to the organisation and the schemes it administers.
3. The Plan complies with the requirements of the Commonwealth Fraud Control Framework (2017).

## Scope

4. This plan applies to all Comcare officials including all ongoing and non-ongoing employees and contractors. in performing Comcare functions.

## Principles

5. This Plan is underpinned by the following principles:
  - a. We are committed to meeting public expectations of integrity, accountability, independence, transparency and professionalism.
  - b. We require Comcare officials to act in accordance with the APS Code of Conduct and Comcare's values to prevent, detect and deal with fraud and corruption against Comcare.
  - c. Comcare will follow Commonwealth fraud guidance and fraud policy as good practice in meeting the requirements of the fraud rule<sup>1</sup>.

---

<sup>1</sup> Comcare must comply with the fraud rule. While not bound by the Commonwealth Fraud Control Policy or Commonwealth fraud guidance, both documents are good practice for Corporate Commonwealth entities.

## DEFINITION OF FRAUD AND CORRUPTION

### Fraud

6. Fraud against the Commonwealth is defined in the Commonwealth Fraud Control Framework (2017) (the Framework) as: 'dishonestly obtaining a benefit, or causing a loss, by deception or other means'<sup>2</sup>.
7. The element of dishonesty means an act of fraud requires more than carelessness, accident or error; it requires deliberate intent. Fraud must also lead to a direct or indirect benefit to an individual or group or to cause a loss. A benefit is not restricted to monetary or material benefits, it also includes intangible benefits such as the unauthorised access to, or disclosure of, sensitive information.
8. Fraud can occur internally, where fraud is committed by Comcare officials. It can also occur externally, where fraud is committed by an individual or group outside of Comcare including, clients and service providers.
9. Fraud may include:
  - a. accounting fraud (e.g. false invoices)
  - b. misuse of Commonwealth credit cards
  - c. misuse of Commonwealth assets, equipment or facilities
  - d. wrongfully using Commonwealth information or intellectual property
  - e. claimants or service providers providing false or misleading information
  - f. claimants not declaring changes in circumstances such as secondary employment or secondary income
  - g. claimants and service providers submitting false invoices for services
  - h. claimants embellishing or misrepresenting the nature or severity of their injury.

### Corruption

10. Comcare has adopted the definition of corruption used by the Australian Public Service Commission (APSC) which is: 'the dishonest or biased exercise of Commonwealth public official functions'<sup>3</sup>.
11. Examples of corruption include:
  - a. bribe-seeking, bribe-giving or bribe-receiving which may relate to a specific decision or action by the receiver
  - b. a serious conflict of interest involving a Comcare official acting in their self-interest, contrary to the interests of Comcare
  - c. collusion or conspiracy between a Comcare official and an external party to inappropriately advance that party's interests, or
  - d. nepotism or cronyism in recruitment, procurement or other processes.

---

<sup>2</sup> [Commonwealth Fraud Control Framework 2017 \(ag.gov.au\)](https://www.ag.gov.au)

<sup>3</sup> <https://www.apsc.gov.au/state-service/state-service-report-2014-15/section-5-aps-values-and-promoting-integrity>

## LEGISLATION AND COMMONWEALTH FRAUD CONTROL FRAMEWORK

12. The Commonwealth Fraud Control Framework 2017 (the Framework) outlines the Australian Government's requirements for fraud control. This includes the need for government entities to implement prevention, detection, investigation and reporting strategies. The Framework, and other Commonwealth fraud control guidance materials, are managed by the Commonwealth Fraud Prevention Centre within the Attorney- General's Department.
13. Within this Framework is section 10 of the Public Governance, Performance and Accountability Rule 2014 (the Fraud Rule): 'The accountable authority of a Commonwealth entity must take all reasonable measures to prevent, detect and deal with fraud relating to the entity.'
14. The Framework also includes the Commonwealth Fraud Control Policy (the Fraud Policy), and Resource Management Guide No. 201 – Preventing, Detecting and Dealing with Fraud (the Fraud Guidance).
15. As a Corporate Commonwealth entity under the PGPA Act, Comcare must comply with the Fraud Rule. While non-binding, as better practice, Comcare follows the other framework documents, the Fraud Policy and Fraud Guidance.

## FRAUD AND CORRUPTION CONTROL FRAMEWORK

16. Comcare's fraud and corruption control framework is consistent with Commonwealth legislative requirements and is underpinned by Comcare's:
  - a. plan and strategies for fraud and corruption
  - b. fraud risk assessments
  - c. culture and values.

### Strategies

17. Comcare has implemented a suite of prevention, detection and response strategies to manage its fraud and corruption risks. Comcare regularly reviews the effectiveness of these strategies to ensure Comcare's approach remains appropriate, cost-effective and proportionate to its risk profile.

### Prevention

18. Prevention is the first line of defence and includes proactive strategies designed to manage the sources of the risk to decrease the likelihood of the risk occurring. Key fraud prevention strategies include:
  - a. organisational culture
  - b. fraud and corruption awareness training
  - c. system and process controls
  - d. regular risk assessments and reviews of treatment strategies.

## Detection

19. Detection measures are designed to uncover instances of fraud and corruption when they occur. Early detection is an essential element of fraud control. Key fraud detection strategies include:
- officials' vigilance during business as usual (BAU) activities
  - monitoring and reporting processes
  - quality assurance checks
  - data analysis and matching activities
  - internal audits and reviews
  - reporting mechanisms to receive both internal and external fraud allegations.

## Response

20. Response activities include an assessment of all reports and allegations to determine an appropriate response. This may include further investigation, analysis, referral, prosecution and recovery. Key fraud response strategies include:
- pursuing disciplinary, administrative, civil or criminal actions as appropriate
  - pursuing the recovery of fraudulently or criminally obtained benefits where appropriate
  - referral to law enforcement bodies as required.

## Risk assessments

21. Regular assessment of risk is critical to preventing and detecting fraud and corruption. In alignment with the Framework, fraud and corruption risk assessments are conducted at least every two years, or when there is a substantial change to Comcare's structure, business operations, functions or activities. Comcare's approach to identifying and controlling fraud and corruption risks aligns with Comcare's overall approach to risk management as outlined in the Risk Oversight and Management Policy and the Risk Management Procedural Guide.
22. Comcare maintains an Enterprise Fraud and Corruption Risk Register with subsidiary detailed Group level Fraud Risk Registers. These are reviewed and assessed on a biannual basis to ensure that they remain current, treatments are progressed and alignment between the documents is maintained.

## Fraud risk appetite

23. Comcare acknowledges that in its interactions with its stakeholders, and in the delivery of its services, all fraud and corruption risks cannot be avoided or prevented. While it is understood that risk cannot be completely avoided, there is no appetite for instances of fraud and corruption which would be considered an offence under the *Criminal Code Act 1995*. Comcare's fraud detection measures will focus on identifying these cases and investigations will be undertaken to obtain evidence to prosecute.
24. Comcare will manage fraud and corruption risks in accordance with its risk appetite, as set out in the *Comcare Risk Management procedure*:
- 'There is no appetite for internal fraud and corruption and the risk may only be accepted where all legislative fraud control requirements are in place and the risk has been reduced to the point where additional controls have negative cost/benefit.
  - There is a low appetite for external fraud against Comcare's programs and the risk may only be accepted where all legislative fraud control requirements are in place and the risk has been reduced to the point where additional controls have negative cost/benefit.'



## Culture and values

25. The APS values, employment principles and code of conduct underpin Comcare's culture and values. All officials must behave in a way that upholds and meets the standards of conduct in line with the APS and Comcare's values.
26. If an employee is suspected of breaching the code of conduct, Comcare will deal with the potential breach in accordance with the Code of Conduct Procedure.

## REPORTING FRAUD AND CORRUPTION

### Reporting by Comcare officials

27. All Comcare officials have an obligation to report incidents of suspected fraud or corruption. All reports remain confidential, however, mechanisms are in place to report the matter anonymously and the Public Interest Disclosure (PID) scheme offers further protections.
28. Comcare officials that suspect that fraud, corruption or misconduct has occurred, should maintain confidentiality and where appropriate discuss the matter with their manager in the first instance. Comcare officials should report fraud matters through the approved channels:
  - a. Claims management matters relating to allegations of fraud by injured employees and/or service providers should, be discussed with their manager in the first instance. The matter can then be reported to the Claims Compliance unit by contacting the Director Claims Strategy and Governance or Assistant Director Claims Compliance and Assurance. The Claims Compliance and Assurance team works with the Fraud Investigation unit to ensure all matters reported or identified are risk assessed and where appropriate, referred on to the Fraud Investigation unit in accordance with the Fraud Allegation Assessment Framework.
  - b. All other matters should be reported to the Fraud Investigation unit by emailing [fraud@comcare.gov.au](mailto:fraud@comcare.gov.au).
  - c. Filling out the Report Fraud online form on the Comcare website. Comcare officials can provide contact details so an investigator can contact them or choose to remain anonymous.
29. Comcare will treat all information relating to evidence or suspicions of fraud, corruption and the identity of the person disclosing this information in confidence.

### Reporting by external stakeholders

30. Comcare provides a range of channels for stakeholders to report behaviour that demonstrates a person or organisation has committed fraud against Comcare or is corrupt. These include:
  - a. filling out the Report Fraud online form on the Comcare website
  - b. email [fraud@comcare.gov.au](mailto:fraud@comcare.gov.au).
  - c. call Comcare directly on 1300 366 979 between 8.30 am and 5.00 pm AEST Monday to Friday
  - d. write to Comcare, GPO Box 9905, Canberra ACT 2601
  - e. stakeholders can ask to remain anonymous and Comcare's investigators will not disclose their identity in their handling of the report.
31. Further information is available on the Comcare website ([www.comcare.gov.au](http://www.comcare.gov.au)).

## MONITORING AND REPORTING

32. Comcare collects information on instances of fraud and corruption (or suspected fraud and corruption) against Comcare. This information includes statistical data, matters under investigation, completed matters, whether the fraud/corruption was proven or not, and whether the matter was dealt with by a criminal, civil or administrative response.
33. The Executive, the Audit and Risk Committee, and the Comcare Enforcement and Fraud Committee are advised of all fraud and corruption investigation outcomes, and the Annual Report includes required reporting information.
34. Comcare provides the Australian Institute of Criminology (AIC) with data on fraud and corruption each year in accordance with s10 of the Public Governance, Performance and Accountability Rule 2014.
35. Comcare will review the Plan every two (2) years as a minimum, or as required in line with changes to the Framework and Comcare's fraud risk assessments.

## SUPPORTING INFORMATION

### Definitions

Term/ Phrase	Definition
AFP	Australian Federal Police
AGIS	Australian Government Investigations Standards
AIC	Australian Institute of Criminology
ANAO	Australian National Audit Office
CDPP	Commonwealth Director of Public Prosecutions
Comcare officials	Comcare employees and contractors
Corruption	The dishonest or biased exercise of Commonwealth public official functions.
Fraud	Dishonestly obtaining a benefit, or causing a loss, by deception or other means.
Fraud Guidance	Attorney-General's Department's Resource Management Guide No. 201 – Preventing, Detecting and Dealing with Fraud
Fraud Policy	Commonwealth Fraud Control Policy
Fraud Rule	Section 10 of the <i>Public Governance, Performance and Accountability Rule 2014</i>
PGPA Act	<i>Public Governance, Performance and Accountability Act 2013</i>
PID	Public interest disclosure
PID Act	<i>Public Interest Disclosure Act 2013</i>
SRC Act	<i>Safety, Rehabilitation and Compensation Act 1988</i>
SRCC	Safety, Rehabilitation and Compensation Commission
WHS Act	<i>Work Health and Safety Act 2011</i>

## Roles and responsibilities

Role	Responsibilities
<b>Accountable Authority</b>	The Chief Executive Officer (CEO), as the Accountable Authority, is responsible for the corporate governance of Comcare and has overall responsibility for fraud and corruption control as well as ensuring compliance with the Framework.
<b>General Managers</b>	Comcare's General Managers have an overarching responsibility for understanding Comcare's fraud risks and promoting fraud control within Comcare. They provide leadership to officials in managing fraud and corruption risks, ensure Comcare's business activities are designed and implemented to effectively prevent and detect fraud and corruption, and to promote ethical behaviour.
<b>Comcare Executive Committee</b>	The Comcare Executive Committee is responsible for oversight of Comcare's Fraud Control Framework and approval of Comcare's Fraud Control Policy.
<b>Audit and Risk Committee (ARC)</b>	The Audit and Risk Committee provides independent assurance and assistance to the CEO on Comcare's risk, control and compliance framework, and Comcare's external accountability responsibilities. Significant findings from fraud risk assessments are reported to the Committee including the progress of implementing treatments. The Committee also receives reports regarding fraud investigations and significant outcomes.
<b>Comcare Enforcement and Fraud Committee</b>	The Comcare Enforcement and Fraud Committee maintains oversight of Comcare's fraud investigations. The Committee is responsible for approving the referral of matters for prosecution to the Commonwealth Director of Public Prosecutions.
<b>Operations Committee</b>	The Operations Committee provides oversight and monitors the Fraud Control related risk assessments and approves the Fraud Control Plan.
<b>Finance and Assurance Team</b>	Finance and Assurance team develop Comcare's fraud control framework and support Comcare officials in implementing strategies to prevent, detect and respond to Fraud and Corruption. The team also assesses allegations of fraud and corruption, undertakes investigations where there is evidence allegations could be a considered an offence under the Criminal Code Act 1995, and refers matters to the relevant law enforcement agency or regulatory body where other offences may have occurred.
<b>Managers and Supervisors</b>	Comcare managers and supervisors must understand the fraud risks in their business area and ensure compliance with policies and procedures and to support implementation of controls. They should promote fraud awareness and ethical behaviours within their business area. Comcare managers and supervisors are responsible for setting an example of sound financial and governance practices, providing consistent communication of Comcare's position on fraud and corruption, and exhibiting a genuine and strong commitment to fraud control to Comcare's officials.
<b>Officials (all levels)</b>	Comcare officials must consider the need to prevent and detect fraud and corruption as part of their normal responsibilities, ensure the effective operation of fraud and corruption treatments relating to their duties, and report instances of fraud and corruption, suspected fraud and corruption or potential weaknesses in risk treatments through appropriate channels.

## Related legislation, procedures, and guidelines

Document name	Link
Public Governance, Performance and Accountability Rule 2014	<a href="#"><i>Public Governance, Performance and Accountability Rule 2014</i></a>
<i>Crimes Act 1914</i>	<a href="#"><i>Crimes Act 1914</i></a>
<i>Criminal Code Act 1995</i>	<a href="#"><i>Criminal Code Act 1995</i></a>
<i>Public Interest Disclosure Act 2013 (PID Act)</i>	<a href="#"><i>Public Interest Disclosure Act 2013</i></a>
The Fraud Rule (section 10 of the Public Governance, Performance and Accountability Rule 2014)	<a href="#"><i>Section 10 – Preventing, detecting and dealing with fraud.</i></a>
Commonwealth Fraud Control Framework including the Resource Management Guide No. 201, Preventing, detecting and dealing with fraud	<a href="#"><i>Commonwealth Fraud Control Framework</i></a>
Australian Government Investigation Standards	<a href="#"><i>Australian Government Investigation Standards</i></a>
Australian Public Service Code of Conduct	<a href="#"><i>APS Values and Code of Conduct</i></a>
Commonwealth Risk Management Policy	<a href="#"><i>Commonwealth Risk Management Policy</i></a>
Accountable Authority Instructions 1 – Corporate Governance	<a href="#"><i>Accountable Authority Instructions 1 – Corporate Governance</i></a>
Comcare Fraud Control Policy	<a href="#"><i>Fraud Control Policy</i></a>
Comcare Compliance and Enforcement Policy	<a href="#"><i>Comcare Compliance and Enforcement Policy</i></a>
Comcare Risk Management Policy	<a href="#"><i>Comcare Risk Management Policy</i></a>
Comcare Assurance Policy	<a href="#"><i>Comcare Assurance Policy</i></a>
Public Interest Disclosures	<a href="#"><i>Public Interest Disclosures</i></a>
Comcare Code of Conduct Procedure	<a href="#"><i>Code of Conduct Procedure</i></a>
Fraud Allegation Assessment Framework	<a href="#"><i>Request via <a href="mailto:fraud@comcare.gov.au">fraud@comcare.gov.au</a></i></a>

## Related training

Document name	Link
Corporate Fundamentals: Fraud Awareness	<a href="#"><i>Via ComLearn</i></a> <a href="#"><i>Corporate Fundamentals: Fraud Awareness</i></a>
Corporate Fundamentals: APS Values and Principles	<a href="#"><i>Via ComLearn</i></a> <a href="#"><i>Corporate Fundamentals: APS Values and Principles</i></a>

## Change history

Version	Date	Author	Reason for change
0.1	21 October 2021	s 47F	Review and update to align with Governance Framework

## Approval and review details

Document Reference	DOC6081588
Document Version Number	0.1
Plan Owner	Chief Operating Officer
Responsible Business Area	Finance and Assurance
Underpinning Policy Name	Fraud Control Policy
Superseded Plan	Fraud Control Policy and Plan 2020 -2022, 21 July 2020
Approved By	Operations Committee
Date Approved	21 October 2021
Date Effective	21 October 2021
Next Review Date	30 June 2024



Australian Government

Comcare

# ***RISK OVERSIGHT AND MANAGEMENT POLICY***

CM9 Document Reference	<i>DOC6539471</i>
Document Version Number	<i>0.3</i>
Policy Owner	Chief Operating Officer
Responsible Business Area	Finance and Assurance
Superseded Policies	Risk Oversight and Management Policy 0.2 5 July 2022
Approved By	Chief Operating Officer
Date Approved	<i>26 September 2023</i>
Date Effective	<i>26 September 2023</i>
Next Review Date	<i>26 September 2024</i>

## CONTENTS

Introduction .....	3
Purpose .....	3
Scope .....	3
Principles .....	3
Policy statement .....	3
Supporting information .....	4
Definitions.....	4
Related legislation .....	5
Related policy, procedures and guidelines .....	5
Change history .....	6

## INTRODUCTION

Section 16(a) of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act) requires that the Accountable Authority of a Commonwealth entity establish and maintain an appropriate system of risk oversight and management for the entity. Accountability and responsibility for Comcare's risk management policy and framework lies with the CEO (as the 'accountable authority').

## Purpose

The purpose of this policy is to confirm and communicate Comcare's commitment and approach to effective risk management. This is to implement a single framework that will contribute to strong management practices and well-informed decision-making. Embedding risk management into our culture and business operations will ultimately contribute to the achievement of our key activities and improved organisational performance.

## Scope

This policy applies to all Comcare officials and contractors, projects, and activities including our activities supporting the Safety, Rehabilitation and Compensation Commission and the Seacare Authority.

Everybody in Comcare is responsible for managing risk.

## Principles

This policy is underpinned by the following principles:

- We are committed to meeting public expectations of integrity, accountability, independence, transparency and professionalism.
- We are committed to following Commonwealth good practice with respect to Risk Management.<sup>1</sup>
- We are committed to effectively managing risk and to using risk management to help inform our decisions for achieving our objectives.

## Policy statement

Comcare will ensure that systematic and effective consideration is given to risks and that risk management is an integral part of effective and well-informed management, planning and decision making.

Specifically, Comcare officials will ensure that:

- a. risk management is undertaken in line with the Comcare Risk Management Framework
- b. risk management is incorporated into corporate, business and operational planning processes
- c. a positive risk culture is promoted where risks are identified early and managed in a timely manner

---

<sup>1</sup> This is in line with paragraph 6 of the Commonwealth Risk Management Policy - "Corporate Commonwealth entities are not required to comply with the Commonwealth Risk Management Policy, but should review and align their risk management frameworks and systems with this policy as a matter of good practice"



- d. annual risk management training is completed
- e. risks are identified, managed, reviewed and monitored regularly
- f. risks are assessed against Comcare's predefined risk assessment criteria and against predefined definitions of likelihood and consequence
- g. risk assessments are undertaken on all new projects to ensure alignment with Comcare's risk appetite and tolerance
- h. a responsible officer is assigned as risk owner for all identified risks to monitor and ensure that appropriate controls and strategies are in place to manage those risks
- i. shared risks that may arise with other entities are identified and managed.

## SUPPORTING INFORMATION

### Definitions

Term/ Phrase	Definition
Accountable Authority	The person or group of persons who has responsibility for, and control over, a commonwealth entity's operations. For Comcare, this is the Chief Executive Officer (CEO).
Consequence	The outcome or impact of an event which may be expressed qualitatively or quantitatively. There can be more than one consequence from one event. Consequences can be positive or negative. Consequences are considered in relation to the achievement of objectives.
Contractors	For the purposes of this policy, a contractor is any person engaged directly or indirectly under a contract for services who has access to create, alter, or remove information, documents, or decision records from Comcare systems.
Control	A measure to modify risk. Controls include any policy, process, device, practice or other actions designed to modify risk.
Likelihood	General description of probability or frequency. It can be expressed qualitatively or quantitatively.
Risk	The effect of uncertainty on objectives. An effect is a deviation from the expected — positive and/or negative. Risk is often expressed in terms of a combination of the consequences of an event and the associated likelihood of occurrence.
Risk Appetite	The amount of risk an entity is willing to accept or retain in order to achieve its objectives. It is a statement or series of statements that describes the entity's attitude toward risk taking.
Risk assessment	The process of risk identification, risk analysis and risk evaluation.
Risk criteria	Terms of reference against which the significance of a risk is evaluated.

Risk culture	Refers to the set of shared attitudes, values and behaviours that characterise how an entity considers risk in its day-to-day activities. A positive risk culture promotes an open and proactive approach to managing risk that considers both threat and opportunity and is one where risk is appropriately identified, assessed, communicated and managed across all levels of the entity.
Risk management	Coordinated activities to direct and control an organisation with regard to risk.
Risk Management Framework	A set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation.
Risk tolerance	The levels of risk taking that are acceptable in order to achieve a specific objective or manage a category of risk. Risk tolerance defines the limits (quantifiable where practicable) that support the entity's risk appetite.
Shared risk	Shared risks arise where a single entity does not manage all the risk on their own. Shared risks are risks where the effect of uncertainty extends beyond a single entity, requiring high levels of cooperation between stakeholders.

## Related legislation

Document name	Link
<i>Public Governance, Performance and Accountability Act 2013</i> <i>Section 16(a) Duty to establish and maintain an appropriate system of risk oversight and management for the entity</i>	<a href="#"><u>Public Governance, Performance and Accountability Act 2013</u></a>

## Related policy, procedures and guidelines

Document name	Link
<i>Commonwealth Risk Management Policy</i>	<a href="#"><u>Commonwealth Risk Management Policy</u></a>
<i>Resource Management Guide No 211: Implementing the Commonwealth Risk Management Policy – Guidance</i>	<a href="#"><u>Resource Management Guide No 211</u></a>
<i>Comcare Accountable Authority Instructions</i>	<a href="#"><u>Accountable Authority Instructions</u></a>
<i>Comcare Risk Management Procedure</i>	<i>Comcare Risk Management Procedure</i>
<i>Comcare risk management ComNet page</i>	<a href="#"><u>Risk Management</u></a>
<i>Comcare risk management register templates</i>	<a href="#"><u>Risk Management</u></a>

## Change history

Version	Date	Author	Reason for change
0.1	6 July 2021	s 47F	Update of content within the new policy template
0.2	1 July 2022		Inclusion of annual training requirement
0.3	26 September 2023		Annual review and update of links to resources



Australian Government

Comcare

## ***RISK MANAGEMENT PROCEDURE***

CM9 Document Reference	DOC6539401
Document Version Number	0.5
Procedures Owner	Chief Operating Officer
Responsible Business Area	Finance and Assurance
Superseded Procedures	Risk Management Procedure 0.4, 4 August 2023
Approved By	Chief Operating Officer
Date Approved	26 September 2023
Date Effective	26 September 2023
Next Review Date	26 September 2024

## CONTENTS

Introduction .....	3
Purpose .....	3
Scope .....	3
Principles .....	3
Risk management framework.....	4
Approach to risk management.....	5
Definitions.....	6
Benefits of managing risk .....	6
Risk management governance.....	7
Emerging risk .....	8
Embedding risk management.....	8
Risk management culture .....	8
Risk appetite and tolerance.....	9
Risk management capability .....	9
Shared risk.....	9
Review of the framework.....	10
Supporting information .....	11
Definitions.....	11
Roles and responsibilities.....	12
Related legislation .....	15
Related policy, procedures and guidelines .....	15
Related training .....	16
Change history .....	16
Attachment A - Risk management process.....	17
Appendix 1 - Comcare risk assessment criteria .....	25
Appendix 2 - Risk tools .....	28
Attachment B - Comcare risk registers and reporting.....	29
Attachment C - Risk appetite and tolerance .....	31
Attachment D - Risk capabilities.....	34
Attachment E - Shared risk .....	35



# INTRODUCTION

## Purpose

This procedure supports Comcare's Risk Management Framework and details the approach required for officials to effectively manage risk. This is to implement a single framework that will contribute to strong management practices and well-informed decision-making. Embedding risk management into our culture and business operations will ultimately contribute to the achievement of our key activities and improve organisational performance.

## Scope

The procedure applies to all Comcare officials and contractors, projects and activities including our activities supporting the Safety, Rehabilitation and Compensation Commission and the Seacare Authority.

Everybody in Comcare is responsible for managing risk.

## Principles

This procedure is underpinned by the following principles:

- We are committed to meeting public expectations of integrity, accountability, independence, transparency and professionalism.
- We are committed to following Commonwealth good practice with respect to Risk Management.<sup>1</sup>
- We are committed to effectively managing risk and to using risk management to help inform our decisions for achieving our objectives.

---

<sup>1</sup> This is in line with paragraph 6 of the Commonwealth Risk Management Policy - "Corporate Commonwealth entities are not required to comply with the Commonwealth Risk Management Policy, but should review and align their risk management frameworks and systems with this policy as a matter of good practice."

## RISK MANAGEMENT FRAMEWORK

### Aim:

To ensure that systematic and effective consideration is given to risks and that risk management is an integral part of effective and well-informed management, planning and decision making in Comcare.

### Policy:

Specifically, Comcare officials will ensure that:

- a. risk management is undertaken in line with the Comcare Risk Management Framework
- b. risk management is incorporated into corporate, business and operational planning processes
- c. a positive risk culture is promoted where risks are identified early and managed in a timely manner
- d. annual risk management training is completed
- e. risks are identified, managed, reviewed and monitored regularly
- f. risks are assessed against Comcare's predefined risk assessment criteria and against predefined definitions of likelihood and consequence
- g. risk assessments are undertaken on all new projects to ensure alignment with Comcare's risk appetite and tolerance
- h. a responsible officer is assigned as risk owner for all identified risks to monitor and ensure that appropriate controls and strategies are in place to manage those risks
- i. shared risks that may arise with other entities are identified and managed.

Comcare's Risk Management Framework has been developed based on the *Public Governance, Performance and Accountability Act 2013* (PGPA ACT), Commonwealth Risk Management Policy<sup>2</sup>, other relevant legislation, and the international standard for risk management ISO 31000:2018, Risk management - Guidelines.

Figure 1 provides a snapshot of the different elements that comprise the framework, including the policy, procedure and guidance documentation, together with the various levels of risk assessment across Comcare, and our risk capability building program.

---

<sup>2</sup> See above



Figure 1: Comcare's Risk Management Framework

## Approach to risk management

Comcare's approach to managing risk is in accordance with the process outlined in the international risk management standard (AS/NZS ISO 31000:2018)

There are five parts in the risk management process:

1. Establish the scope
2. Risk identification
3. Risk analysis
4. Risk evaluation
5. Risk treatment.

Each part is supported by communication, monitoring and review, and recording and reporting. While the process is described in 'parts', it is not a linear box-ticking exercise, but continuous and iterative.

Further details on this process and the supporting criteria are provided at [Attachment A](#).

The objective of effective risk management is to minimise the effect of uncertainty, enabling improved organisational performance. As a national leader in work health and safety, Comcare faces a broad range of risks, including from its responsibilities as an insurer, regulator, and scheme manager, as well as from day-to-day operational activities.

Comcare is committed to effectively managing risk in all activities, and to using risk management to help inform all decisions. This includes recognising that risk can have both positive (opportunities) and negative (threats) impacts on the business. Our approach to risk management focuses on identifying and leveraging positive impacts and events, while continuing to be mindful of potential negative consequences, along with compliance and budgetary requirements.



Comcare has embedded a structured, consistent and comprehensive approach to risk management as part of its governance and planning processes, and organisational culture. Risk management is considered an integral element of good management. Part of this is a culture of continual improvement, with a focus on:

- a. improving understanding and evaluation of control effectiveness
- b. establishing a high-quality agency-wide risk management framework
- c. providing comprehensive training and development on risk
- d. evaluating and improving risk performance, and
- e. strengthening engagement with stakeholders on risk-related matters.

## Definitions

Risk is defined as the effect of uncertainty on objectives. Risk is often characterised by reference to potential events and the consequence (or impact) that may flow from it. Risk is measured in terms of a combination of the consequence of an event and its likelihood of occurrence. Generally, the causes of risk are almost exclusively people, process, procedures or natural events.

Risk is inherent in everything that Comcare does: implementing Government policy; acting as a regulator; its role as an insurer; managing the scheme; managing a project; dealing with stakeholders; determining work priorities; establishing safe methods of work; or purchasing new goods or services.

Risk management is a systematic approach of identifying, assessing and responding to risks to support better decision making.

Risk management is an ongoing process that is applied to all our activities. It is an integral part of management and decision making and is an essential part of planning each new area of work, project or policy initiative. Ideally risk assessment and management is undertaken prior to new work commencing to ensure it is structured and resourced in the most appropriate way and continues throughout the life of the activity.

The aim of risk management is not to eliminate all risk, but rather to effectively manage the risks involved in Comcare's activities by introducing effective controls and mitigation strategies.

## Benefits of managing risk

The key benefit of effectively managing risk within Comcare is to ensure delivery of Government policy and our objectives, in a structured and comprehensive manner. This helps us avoid surprises and helps future proof our activities.

Some specific benefits include:

- a. improved accountability
- b. protection of Comcare's reputation
- c. better informed decision-making
- d. improved financial management and performance
- e. better allocation and use of public resources
- f. improved health and safety
- g. better protection and management of Comcare's assets, and
- h. better protection of Comcare from legal liability.

Comcare's risk management [ComNet page](#) and our whole-of-agency risk familiarisation and training sessions are also critical for building our positive risk culture.

## Risk management governance

Comcare has three tiers of risk ordered as strategic, operational, and group risk. This aligns with the [Governance Committee Structure](#) shown in Figure 2.

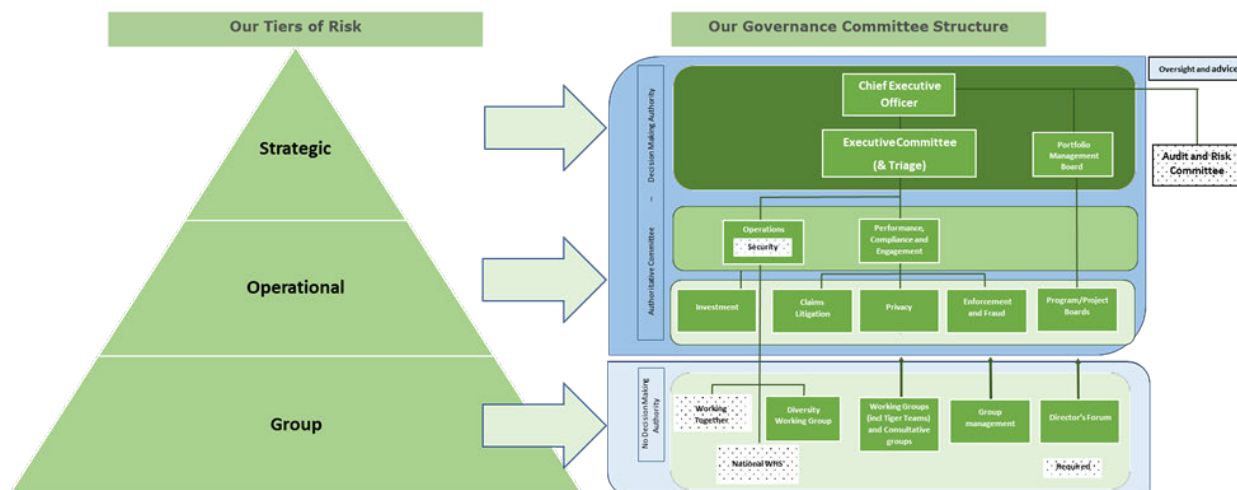


Figure 2: Tiers of risk alignment to governance committee structure

This alignment model represents the different levels of risk and the designated level of oversight as per each of the committee charters or terms of references.

**Strategic Risk:** At the highest level, the Executive Committee provides strategic oversight and guidance of Comcare's overall performance and accountability requirements including our risk management framework, policy, plans and registers covering the strategic and emerging risks. The Audit and Risk Committee provides independent, external assurance of the system of risk management.

**Operational Risk:** At the operational level, the three authoritative committees play a role as per their respective terms of reference with monitoring the management of Comcare wide operational risks, supporting management plans and registers relating to their areas of oversight. These committees are the Operations Committee, the Performance, Compliance and Engagement (PCE) Committee and the Portfolio Management Board (PMB). These authoritative committees can make decisions on strategy, priorities and set of works within the relevant area of responsibility and still remain accountable to the Executive Committee for these decisions. In line with the approved terms of reference, extreme risks are required to be escalated to the Executive Committee.

The timings of review and reporting vary according to the type of framework and compliance requirements and are captured as separate agenda items in each of the Committees agenda schedules.

**Group Risk:** At the group level, each group is responsible for monitoring and maintaining their respective risk registers in line with their business planning processes. Where groups identify high or extreme risks relevant to Comcare's operational or strategic risks, they should escalate the risks through the appropriate operational area and Authoritative Committee.

The risk registers and reporting requirements associated with these tiers of risk is provided at [Attachment B](#).

## Emerging risk

Emerging risks are newly developing or evolving risks on the horizon that can affect the achievement of an organisation's strategic objectives. It may be difficult to fully articulate or assess their likelihood or consequence, given they are newly developing and may not yet have a track record to analyse. It is important Comcare consider these risks to better identify and prepare for possible disruptions and build resilience. This also creates a mechanism to provide early warning to the executive and enables them to put in place appropriate measures and controls.

The Chief Operating Officer (COO) is responsible for oversight of the process for identifying, managing, escalating and closing off emerging risks affecting the Comcare business (including considering of how they may fit in to Comcare's risk reporting). Emerging risks can be raised verbally, via email or through multiple sources but will be brought to Executive's attention through regular reporting to the Executive Committee (EC). All Groups through their annual planning activities, director meetings, collaboration and forums will identify emerging risks. Corporate Group will engage with the Audit and Risk Committee secretariat and all Comcare Groups to collate the emerging risks in the Emerging Risk Register for reporting and discussion. Corporate Group will prepare the discussion paper and present this to the EC, at regular intervals following Audit and Risk Committee meetings. The emerging risks process is shown in Figure 3. Further guidance on the emerging risk process is on Comcare's risk management [ComNet page](#).

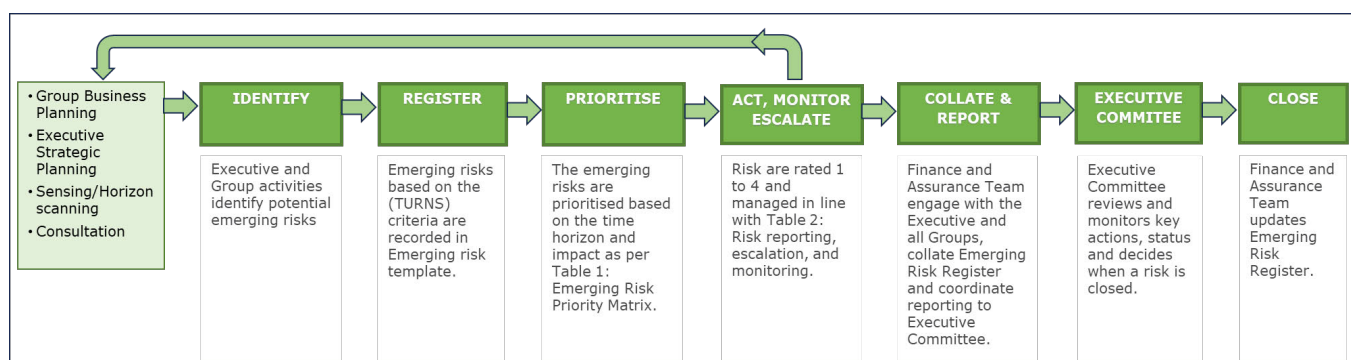


Figure 3. Emerging risk process

## Embedding risk management

Risk management is not separate from other business activities, but rather should form part of business-as-usual activities. Risk management considerations and requirements should be integrated into all corporate policies, procedures and guidelines. Where necessary, such policies will also be reflective of where there is a shared risk between Comcare and another organisation.

Key to this integrated approach is the way in which the Comcare Risk Oversight and Management Policy acts in concert with the Comcare Corporate Plan, Group Business Plans, Fraud Control Plan, Business Continuity Manual, WHS Management System and the Security Policy. All mutually strengthen the effectiveness of each other and provide for effective and efficient planning and controls around Comcare's resources and continued operation.

## Risk management culture

The Commonwealth Risk Management Policy defines a positive risk culture as one that 'promotes an open and proactive approach to managing risk that considers both threat and opportunity.' Additionally, the APS Values require a commitment to service and accountability. The Australian Public Service Commissioner's Directions

2016 require APS employees to have regard to their duties and responsibilities, identify and manage areas of potential risk and demonstrate that their actions and decisions reflect appropriate consideration.

Comcare will promote and facilitate a positive risk culture where risks are identified early, and openly, and managed in a way that supports delivery of Comcare's business priorities. Attributes that will lead to a positive risk culture, and that Comcare will continually promote and reinforce, include:

- members of the Executive, directors and supervisors will demonstrate leadership and commitment to ensure risk management is integrated into all Comcare's activities
- risk is considered in all activities, from corporate planning to day-to-day operations
- officials take personal responsibility for the management of risk and proactively seek to involve others when relevant
- officials are comfortable talking openly and honestly about risk using a common risk language, and
- officials are comfortable raising issues and escalating risks.
- accessible risk management information and whole-of-agency risk awareness and mandatory training.

## Risk appetite and tolerance

Comcare recognises that many of its activities have residual risk and that it is not possible or desirable to eliminate all risk.

Comcare's risk tolerance for individual activities and projects will be defined early in their development and communicated to all relevant stakeholders. Comcare has defined its risk appetite and tolerance levels in Attachment C.

## Risk management capability

Comcare recognises that risk management is a key competency and responsibility for all officials. As such, risk management is to be incorporated into our job descriptions, duty statements and performance agreements, as appropriate.

Comcare will maintain an appropriate level of capability to both implement the risk management framework and manage its risks, commensurate with available resources and needs.

Attachment D summarises the capabilities for each APS level, as well as the required training for EL2, EL1 and APS6 officers.

## Shared risk

Comcare has a responsibility not only to manage its own risks, but also identify and manage risks that may come with inter-entity partnerships and similar arrangements.

A shared risk is where the risk involves more than one entity, or where another entity can significantly influence a risk. These risks may extend to other Commonwealth agencies and/or may include the community, industry, international partners and other jurisdictions. Other mechanisms that may lead to a shared risk include memorandums of understanding, treaties, contracts, projects, Government directions or working groups.

If the responsibility for specific controls fall to another party and the effectiveness of these controls is relied on by other parties, then this would be classified as a shared risk.

Comcare shares significant risks with other organisations. These include shared risks as an insurer, along with shared risks in its regulatory functions.

Where a shared risk exists, Comcare will work with the other organisation/s to ensure the organisation best placed to manage that risk does so, subject to any legislative requirements. The CEO expects that officials will seek advice from the relevant General Manager and/or the Executive Committee, if there are circumstances where a shared risk may exist and thus require management. Where a shared risk arises through current or potential contractual arrangements, advice must be sought from the Legal Group.

All shared risks should be identified in the appropriate risk register, either at the operational/project, Group, or whole-of-organisation level.

Comcare cannot abrogate its responsibility to manage shared risk. This applies even where a third party has been recognised to be best placed to manage that risk. In many cases, Comcare will retain responsibility for overseeing how well that third party is managing the risk.

Examples of shared risks and further guidance on how to identify them is provided at [Attachment E](#).

## Review of the framework

Comcare will review the appropriateness and effectiveness of its risk management framework and policy, along with the application of risk management practices within Comcare, annually.

Reviews of the policy, along with the performance of Comcare's risk management framework, will include four key components:

- reviewing Comcare's risk management policy and framework for continued appropriateness and effectiveness
- reviewing compliance with and the application of the framework
- reviewing Comcare's Strategic Risk Register, and
- reviewing the Group risk management plans (including associated risk registers).

There will be ongoing review and evaluation of Comcare's risk management framework by the Finance and Assurance team through:

- management reporting at the Group level
- quarterly reporting to the Executive Committee
- biannual reporting to the Operations Committee
- quarterly reporting to the Audit and Risk Committee
- internal and external audits (when conducted).

Should improvements be identified in the period between formal reviews, depending on the scale of the suggested changes, the changes will require approval in alignment with the [Comcare Governance Documentation and Consultation Procedure](#).

## SUPPORTING INFORMATION

### Definitions

Term/ Phrase	Definition
Accountable Authority	The person or group of persons who has responsibility for, and control over, a commonwealth entity's operations. For Comcare, this is the Chief Executive Officer (CEO).
Consequence	The outcome or impact of an event which may be expressed qualitatively or quantitatively. There can be more than one consequence from one event. Consequences can be positive or negative. Consequences are considered in relation to the achievement of objectives.
Contractors	For the purposes of this policy, a contractor is any person engaged directly or indirectly under a contract for services who has access to create, alter, or remove information, documents, or decision records from Comcare systems.
Control	A measure to modify risk. Controls include any policy, process, device, practice or other actions designed to modify risk.
Hierarchy of controls	This is specific to WHS. A pyramid of steps that should be considered in sequence when evaluating the ways to remove or reduce a discovered risk. Each step in the pyramid should be considered but preference should be given to control measures higher up the hierarchal structure than those at the bottom. The most effective risk control will often also come from implementing a number of levels from the hierarchy simultaneously.
Likelihood	General description of probability or frequency. It can be expressed qualitatively or quantitatively.
Risk	The effect of uncertainty on objectives. An effect is a deviation from the expected — positive and/or negative. Risk is often expressed in terms of a combination of the consequences of an event and the associated likelihood of occurrence.
Risk Appetite	The amount of risk an entity is willing to accept or retain in order to achieve its objectives. It is a statement or series of statements that describes the entity's attitude toward risk taking.
Risk assessment	The process of risk identification, risk analysis and risk evaluation.



Term/ Phrase	Definition
Risk criteria	Terms of reference against which the significance of a risk is evaluated.
Risk culture	Refers to the set of shared attitudes, values and behaviours that characterise how an entity considers risk in its day-to-day activities. A positive risk culture promotes an open and proactive approach to managing risk that considers both threat and opportunity and is one where risk is appropriately identified, assessed, communicated and managed across all levels of the entity.
Risk management	Coordinated activities to direct and control an organisation with regard to risk.
Risk Management Framework	A set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation.
Risk tolerance	The levels of risk taking that are acceptable in order to achieve a specific objective or manage a category of risk. Risk tolerance defines the limits (quantifiable where practicable) that support the entity's risk appetite.
Shared risk	Shared risks arise where a single entity does not manage all the risk on their own. Shared risks are risks where the effect of uncertainty extends beyond a single entity, requiring high levels of cooperation between stakeholders.

## Roles and responsibilities

Role	Responsibilities
Chief Executive Officer	<ul style="list-style-type: none"> <li>Accountable and responsible for Comcare's risk management policy and framework (as the 'accountable authority').</li> <li>Endorse and champion Comcare's risk management framework and policy, ensuring they are appropriate, resourced, and implemented.</li> <li>Determine and articulate Comcare's risk appetite and tolerance.</li> <li>Approve Comcare's strategic risk profile.</li> <li>Establish and maintain an appropriate system of internal controls for Comcare.</li> <li>Report on Comcare's key risks to the responsible minister.</li> </ul>
Risk Champion (Chief Operating Officer)	<ul style="list-style-type: none"> <li>Champion risk management within Comcare, and the Executive.</li> </ul>

Role	Responsibilities
	<ul style="list-style-type: none"> <li>• Ensure the Comcare risk register and risk profile are monitored.</li> <li>• Oversee the implementation of the Comcare Risk Oversight and Management Policy.</li> <li>• Liaison with the Audit and Risk Committee on risk management.</li> <li>• Monitor and communicate risk management performance.</li> </ul>
Executive	<ul style="list-style-type: none"> <li>• Model leadership and commitment to risk management.</li> <li>• Ensure adherence to the Risk Oversight and Management Policy.</li> <li>• Assist the CEO to define overall risk appetite and enterprise risk profile.</li> <li>• Identify and provide controls/treatments for emerging risks.</li> <li>• Approve funding for risk management.</li> <li>• Assure clarity of role and responsibility of other stakeholders.</li> <li>• Review recommendations from the Audit and Risk Committee and other assurance and review activities. Implement improvements as required.</li> </ul>
Group/Business Area/ Programme/ Project Manager	<ul style="list-style-type: none"> <li>• Own and implement the appropriate Risk Management Plan.</li> <li>• Identify, review and manage the risks and risk profiles for their teams, ensuring risk registers, risk review process and escalation process are in place.</li> <li>• Ensure officials are aware of Comcare's risk management framework in their decision making.</li> <li>• Appropriately recognise risk management behaviours (positive or negative) within their teams.</li> <li>• Identify resources to manage/mitigate risk.</li> <li>• Own individual risks (including those delegated by the senior manager)</li> <li>• Escalate or delegate risks to higher or lower levels in the organisation as required.</li> <li>• Ensure participation in the delivery of risk management.</li> <li>• Explicitly identify risk management duties within the terms of engagement of other managers involved in achieving specific objectives.</li> <li>• Communicate emerging risks to appropriate level for immediate mitigation and overall organisational consideration.</li> </ul>
Finance and Assurance	<ul style="list-style-type: none"> <li>• Lead and seek continuous improvement in organisational risk management.</li> </ul>



Role	Responsibilities
	<ul style="list-style-type: none"> <li>• Advise the Executive Committee of appropriate direction for risk management activities.</li> <li>• Assure the Executive/Senior Management Team that risk accountabilities exist.</li> <li>• Implement the risk management framework and maintain the Risk Management Policy and Procedure.</li> <li>• Co-ordinate risk management planning to ensure consistency and accuracy of practice.</li> <li>• Report to the Executive Committee, Audit and Risk Committee and Operations Committee at regular intervals.</li> <li>• Provide guidance and support to all officials on the implementation of the policy and procedure</li> <li>• Develop risk management guidance, support and facilitate risk assessment workshops.</li> </ul>
Risk Owner (EL2s, EL1s, APS6)	<ul style="list-style-type: none"> <li>• Primary point of responsibility for monitoring a specific risk.</li> <li>• Understand the risks they are charged with.</li> <li>• Understand and interpret Comcare's risk appetite and tolerance as it applies to their risks.</li> <li>• Maintain appropriate risk registers by actively monitoring the risk context to understand and respond to any changes, actual or likely.</li> <li>• Identify emerging risks and develop control/treatment options.</li> <li>• Actively challenge control owners and the effectiveness of controls.</li> <li>• Communicate and report on the risk whenever required.</li> </ul>
Officials (all levels)	<ul style="list-style-type: none"> <li>• Participate (as appropriate) in the identification, assessment, planning and management of threats and opportunities</li> <li>• Understand and implement the Risk Oversight and Management Policy within their area of responsibility</li> <li>• Escalate risks as necessary as defined by the relevant risk management plan.</li> <li>• Complete mandatory training on annual basis.</li> </ul>
Audit and Risk Committee	<ul style="list-style-type: none"> <li>• Monitor, review, and provide independent, external assurance and where appropriate, make recommendations to the CEO and the Chairperson of the Seacare Authority with respect to:             <ul style="list-style-type: none"> <li>○ financial reporting</li> <li>○ performance reporting</li> <li>○ system of risk oversight</li> </ul> </li> </ul>

Role	Responsibilities
	<ul style="list-style-type: none"> <li>○ system of internal control</li> <li>○ internal and external audit.</li> <li>• The Committee is not responsible for the executive management of these functions and has no executive powers.</li> </ul>
Operations Committee	<ul style="list-style-type: none"> <li>• Oversight and monitors of specific types of operational risks to assure the CEO that appropriate governance and compliance arrangements are in place for these functions. These risks are managed through specific risk assessments and reporting, and include those areas where there is a legislative, commonwealth framework, regulatory or special requirement, such as Fraud Control, Protective Security, Work Health and Safety, Child Safety and Modern Slavery and COVID-19 Pandemic.</li> </ul>
Performance, Compliance and Engagement (PCE) Committee	<ul style="list-style-type: none"> <li>• Responsible for monitoring those operational risks relating to the cross organisational delivery of Comcare's services, compliance with statutory and regulatory obligations, management of data and stakeholder engagement. The PCE committee is also responsible for assessing our performance, management of complaints and risks arising from non-compliance with statutory obligations or external scrutiny.</li> </ul>
Portfolio Management Board (PMB)	<ul style="list-style-type: none"> <li>• Monitors and reviews identified portfolio, program, project risks, with assurance support provided by the Enterprise Portfolio Management Office (EPMO). This is in accordance with the Portfolio Management Board Terms of Reference.</li> </ul>

## Related legislation

Document name	Link
Public Governance, Performance and Accountability Act 2013 Section 16(a) Duty to establish and maintain an appropriate system of risk oversight and management for the entity	<a href="#">Public Governance, Performance and Accountability Act 2013</a>
Work Health and Safety Act 2011 (Cth)	<a href="#">WHS Act</a>
Work Health and Safety Regulations 2011 (Cth)	<a href="#">WHS Regs</a>

## Related policy, procedures and guidelines

Document name	Link
---------------	------

<i>Commonwealth Risk Management Policy</i>	<a href="#"><u>Commonwealth Risk Management Policy</u></a>
<i>Resource Management Guide No 211: Implementing the Commonwealth Risk Management Policy – Guidance</i>	<a href="#"><u>Resource Management Guide No 211</u></a>
<i>Comcare Accountable Authority Instructions</i>	<a href="#"><u>Accountable Authority Instructions</u></a>
<i>Comcare Risk Oversight and Management Policy</i>	<a href="#"><u>Comcare Risk Oversight and Management Policy</u></a>
<i>Comcare risk management ComNet page</i>	<a href="#"><u>Risk Management</u></a>
<i>Comcare risk management register templates</i>	<a href="#"><u>Risk Management</u></a>
<i>Emerging Risk Process</i>	<a href="#"><u>Risk Management</u></a>
<i>How to manage Work Health and Safety risks Code of Practice 2015</i>	<i>Risk Code of Practice</i>
<i>Work Health and Safety Policy</i>	<i>WHS Policy</i>
<i>WHS risk management fact sheet</i>	<i>WHS fact sheet</i>

## Related training

Document name	Link
<i>Corporate Fundamentals: f Risk Essentials</i>	Via <a href="#"><u>ComLearn</u></a> Corporate Fundamentals: <a href="#"><u>Risk Essentials</u></a>
<i>Corporate Fundamentals: Fraud Awareness</i>	Via <a href="#"><u>ComLearn</u></a> <a href="#"><u>Corporate Fundamentals: Fraud Essentials</u></a>

## Change history

Version	Date	Author	Reason for change
0.1	6 July 2021	s 47F	Review and update to align with Governance Framework
0.2	19 November 2021		Group risk process and risk appetite statement changes
0.3	1 July 2022		Emerging risk, WHS input and minor amendments
0.4	3 August 2023		Update of Risk Appetite and Tolerance Statement
0.5	26 September 2023		Annual update and emerging risk process changes

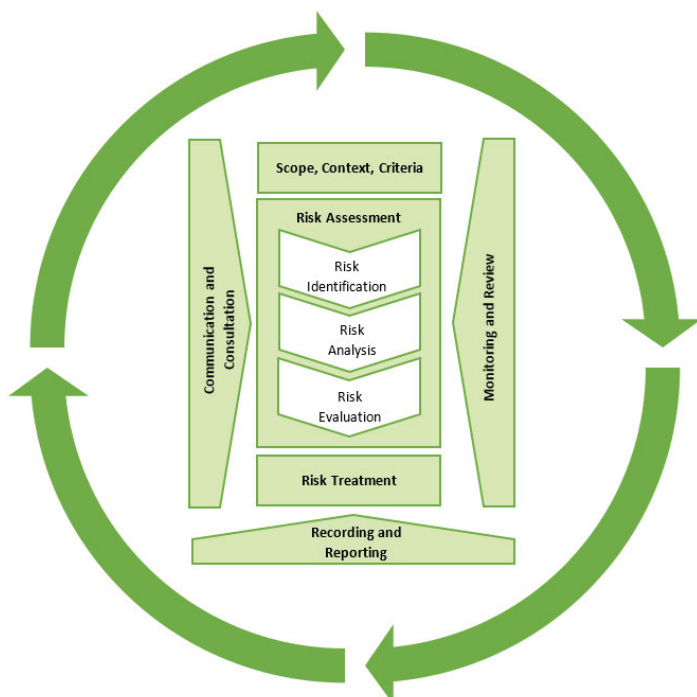


## ATTACHMENT A - RISK MANAGEMENT PROCESS

Comcare's approach to managing risk is in accordance with the process outlined in the international risk management standard (AS/NZS ISO 31000:2018) as shown in Figure 4.

There are five parts in the risk management process. Each part is supported by communication, monitoring and review, and recording and reporting. While the process is described in 'parts', it is not a linear box-ticking exercise, but continuous and iterative.

Figure 4: Comcare's Risk Management Process



**1. Establish the scope, context and criteria.** This involves understanding the risk management process, the objectives and context of your activity, and key stakeholders.

**2. Risk identification.** Identify the risk events, including their causes and potential consequences. This includes both threats and opportunities.

**3. Risk analysis.** Analyse risks in terms of consequences and likelihood whilst estimating the level of risk (see the risk matrix at [Appendix 1, Table 6](#)).

**4. Risk evaluation.** Determine whether the risk is acceptable to Comcare using the risk matrix and any legal, regulatory and other mandatory requirements.

**5. Risk treatment.** For unacceptable risks, identify actions that could be taken to mitigate the risks. The cost and effort must be balanced against the benefits of that risk treatment.

**Monitoring and review:** Identified risks and associated treatments will be monitored, reported, and reviewed for effectiveness regularly.

**Communication and consultation:** Communication and consultation with key internal and external stakeholders at each stage of the risk management process is central to maintaining high levels of confidence.

**Recording and reporting:** Document the results of the risk assessment in Comcare's risk register templates and report the results to management, particularly any unacceptable risks that need to be escalated.

### 1. Establish the scope, context and criteria

#### Why is this important?

The first step in the risk management process helps you understand the environment around your risk assessment. This involves defining the scope of the activity and assessing and understanding the internal and external context. Comcare has defined its appetite and tolerance levels in [Attachment D](#). Other risk criteria are at [Appendix 1](#), with templates provided on the risk management [ComNet page](#).

#### Minimum requirements

Understand the following:

- Comcare’s risk management process (as outlined in this document)
- objectives and decisions related to your activity, including the internal and external context
- expected outcomes of the risk assessment
- resources, roles and responsibilities
- relationships with other projects, processes and activities.

Identify key stakeholders, both internal and external.

### **Tips and traps**

Risks do not operate in a vacuum. You should take the internal and external environment of Comcare and the purpose of the risk management activity into account when you undertake a risk assessment.

The depth of information required for this section relates directly to the size and complexity of the risk management activity being undertaken. The risk assessment template is a good way to capture this information.

For this step, consider:

- Defining the objective in SMART (Specific, Measurable, Achievable, Relevant, Time-bound) terms so that it is clear what success would look like
- Reviewing documentation such as the Comcare Corporate Plan (our principal planning document), Group Business Plans or previous risk assessments, which may help you understand the context of your activity.

## **2. Risk identification**

### **Why is this important?**

The second step in the risk management process is designed to help you identify and document the events (and their causes) that could occur in the internal and external environment established in Step 1, that would impact your objectives. This includes threats and hazards that have the potential to impact the safety and wellbeing of yourself or others. You should consider both negative and positive risks.

### **Minimum requirements**

- Identify risks (positive and negative) that may impact on the objectives from being achieved
- Identify the causes and consequences for each risk
- Identify a risk category for each risk
- Identify a Risk Owner for each risk.

### **Tips and traps**

You can use the categories listed in Table 1 below to help you think through different types of risks. When recording risks in the relevant risk register, you will find that risks can fall into multiple categories. When this happens, you should determine a primary category. To determine a primary category, think about the greatest area of impact from the threat or opportunity.

Capability	Delivery	Reputation
<ul style="list-style-type: none"> <li>Capacity</li> <li>People</li> <li>Financial processes</li> <li>Technology</li> <li>Physical infrastructure</li> <li>Legislative</li> <li>Regulatory</li> <li>Security</li> <li>Safety</li> </ul>	<ul style="list-style-type: none"> <li>Processes</li> <li>Governance</li> <li>Management</li> <li>Resources</li> <li>Compliance</li> <li>Policy</li> <li>Structure</li> <li>Administration</li> <li>Timeliness</li> <li>Quality</li> </ul>	<ul style="list-style-type: none"> <li>Government expectations</li> <li>Stakeholders</li> <li>Communications</li> <li>Implementation</li> <li>Management</li> <li>Delivery</li> <li>Media</li> </ul>

Table 1: Risk categories

A range of tools may be used to identify risks:

- the butterfly or bowtie technique (see [Appendix 2](#))
- fishbone diagrams (see [Appendix 2](#))
- audits or inspections
- analysing strengths, weaknesses, opportunities and threats (SWOT)
- brainstorming
- complaints or incident analysis
- decision trees and process mapping
- researching local and overseas experience
- generating scenarios
- focus groups
- risk workshops, and
- expert advice.

Once a risk is identified it should be given a description that accurately describes the key features of the risk as follows:



It can be helpful to remember that risk descriptions can follow this structure: “Something might occur which {Causes} the {Event} that leads to an {Impact / Consequence}.”

Example 1: The [cause] of [event] leading to [an impact on objectives].

*Software vulnerabilities allows a hacker to breach our ICT systems resulting in a breach of information security and privacy of our clients.*

This could also be written as:

Example 2: The [event] due to [cause] leading to [an impact on objectives].

*A hacker breaches our ICT systems using software vulnerabilities resulting in a breach of information security and privacy of our clients.*

Either way is correct so long as it can be understood.

It is helpful to test the risk description with a person who is not the risk owner. This will help to ensure it can be understood and that it is describing the actual problem.

It is critical in this analysis stage to ensure that the proper risks are identified and that risks are not confused with the causes or impacts.

### 3. Risk analysis

#### Why is this important?

This third step helps you to understand the risk and determine the risk level so that you can make decisions about its acceptability in the next step.

#### Minimum requirements

For each risk, you must determine the current risk level, which is the amount of risk Comcare is facing right now. This takes any existing controls into account.

To assess this, you need to determine:

- Existing controls: This allows you to know what is currently in place to address the causes, detect when a risk is materialising, or mitigate the consequences. This should include identifying Control Owners. You also need to consider how effective these controls are – use [Appendix 1, Table 3](#).
- Control Owner: For each control, identify somebody who is accountable for it.

Once you have a good understanding of the existing controls you can then determine a current level of risk by assessing:

- Consequences: This is the impact if nothing additional (i.e. new controls) is done about the risk. You should think about the risk's potential to impact on Comcare, the Group, project or activity. Use [Appendix 1, Table 4](#).
- Likelihood: The likelihood of the consequence occurring during the life of the objective. You should use information from the previous step on the causes of the risk to help you determine this. This must consider the effect of existing controls. Use [Appendix 1, Table 5](#).
- Risk level: Using the likelihood and consequence selections, you then estimate the current level of risk using the Comcare risk matrix - use [Appendix 1, Table 6](#). The matrix shows the likelihood and consequence axes. The intersection of these axes derives the risk rating.

#### Tips and traps

The rating of risks is a subjective process – some people may see a risk as high, while others may see it as significantly lower. It is important to consult and communicate with stakeholders to obtain a variety of viewpoints to assist in determining a suitable rating.

When recording consequence ratings, if there are multiple consequences, use the highest level.

It can also be useful to think about what types of controls are currently in place to ensure that you are controlling different aspects of the risk. Controls can generally be divided into four categories as shown in Table 2.



Advisory controls	Preventative controls	Detective controls	Corrective/ responsive controls
<p>These are intended to provide information on how to prevent the risk from happening or avoid the risk.</p> <p>For example:</p> <ul style="list-style-type: none"> <li>• Policies and processes</li> <li>• Minimum standards</li> <li>• Duty statements</li> <li>• Training</li> <li>• Warning signs/posters</li> </ul>	<p>These affect a cause of the risk.</p> <p>For example:</p> <ul style="list-style-type: none"> <li>• System access controls</li> <li>• Segregation of duties</li> <li>• Locks and barriers</li> <li>• Security screening</li> <li>• Checks and testing</li> </ul>	<p>These help you be aware of when a risk occurs.</p> <p>For example:</p> <ul style="list-style-type: none"> <li>• Complaint hotlines</li> <li>• Reviews</li> <li>• Reconciliations</li> <li>• Security camera</li> <li>• Automated monitoring</li> <li>• Smoke alarm</li> </ul>	<p>These affect the consequences of the risk. These are rarer than the other three types of controls.</p> <p>For example:</p> <ul style="list-style-type: none"> <li>• Business continuity plan</li> <li>• PR and Media management</li> <li>• Investigation handling procedures</li> <li>• Building fire sprinkler systems</li> </ul>

Table 2: Risk controls

## 4. Risk evaluation

### Why is this important?

This fourth step helps you decide whether each risk is acceptable or not and whether it needs to be treated.

### Minimum requirements

When evaluating a risk, you should use Comcare's risk matrix ([Appendix 1, Table 6](#)), risk escalation, mitigation and monitoring table ([Appendix 1, Table 7](#)) and the risk appetite and tolerance statements, [Attachment D](#) to determine whether it is acceptable or not.

Factors to consider when evaluating risk include:

- The importance of the activity you are assessing in the context of Comcare's objectives and priorities (See Step 1 – Establish the scope, context and criteria)
- The degree of control you have over mitigating the risk
- The potential and actual losses which may arise should the risk occur
- The benefits and opportunities presented by the risk.

### Tips and traps

When evaluating the risk, consider the objectives of Comcare and any constraints imposed by Commonwealth legislation, regulation or whole-of-government policy. All work health and safety (WHS) risks must be reduced 'so far as reasonably practicable'. The hierarchy of control is implemented to achieve this objective using a three-tiered approach to identify possible controls. Refer to the WHS risk management fact sheet.

In some instances, if the risk is acceptable according to Comcare's risk matrix, you may decide to maintain the existing controls and take no further action. In some instances, you may want to introduce further controls as best practice even though the risk level may already be acceptable.

Should a risk be evaluated as exposing Comcare to an intolerable level of risk, it must be treated accordingly.



## 5. Risk treatment

### Why is this important?

Step five is designed to help you develop more effective ways of controlling the risk. Risk treatment is usually only undertaken when the risk is unacceptable with existing controls. Risk treatments should be included if they reduce the likelihood and/or consequence levels, or form part of best practice or compliance activities.

### Minimum requirements

You should:

- Consider the level and responsibilities for treating the risk as indicated in the risk escalation, mitigation and monitoring table ([Appendix 1, Table 7](#))
- Treat any unacceptable risks
- For each risk, determine the residual risk level after treatment if the treatments are implemented effectively. The residual risk level should be tolerable to Comcare
- Consider treatments for shared risks and establish an agreement with other parties as to who is responsible for what and how you may collaborate to reduce the risk level. A Treatment Owner and a plan for implementation should be determined.

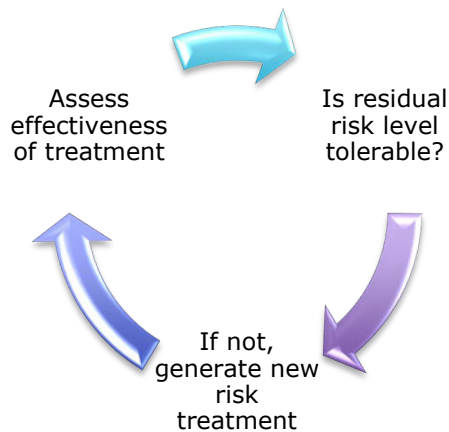
The cost and effort needed to implement a risk treatment must be balanced against the benefits of that risk treatment. Options for risk treatment include:

- Taking the risk if it is a positive risk / opportunity.
- Avoiding the risk by deciding not to start or continue with the proposed activity likely to trigger the risk (where that is practicable)
- Removal of a source of risk
- Changing the likelihood and consequence of the risk through additional controls, thereby changing the risk to an acceptable level
- Retaining, owning or accepting the risk through a deliberate decision
- Sharing the management of the risk, wholly or in part, to another party noting that responsibility for 'duty of care' cannot be transferred and generally, the overarching accountability for the risk cannot be transferred.

### Tips and traps

When selecting the best treatment option, it is essential to compare the benefits of implementing the option with the cost of implementation. The cost to consider is not just financial, as there may also be a resourcing, objective or reputational outcomes to consider in determining the best treatment option.

It can be useful to think about risk treatment as a cycle, where if you determine that a risk needs treatment, you should consider the steps shown in Figure 5 below.



*Figure 5: Risk Treatment Cycle*

## Monitoring and review

### Why is this important?

This is about making sure that risk management isn't a 'set and forget' activity. Reviewing risk assessments regularly will ensure that they are still relevant while reporting progress provides assurance that our objectives are being achieved and ensuring there are no unintended threats or hazards that arise from the treatments implemented.

### Minimum requirements

Ensure there is a plan to regularly examine the risks and controls to make sure nothing has changed. You should monitor and review controls to confirm they are working adequately and effectively to manage the risk, and identify emerging risks and lessons learned to ascertain its effect on proposed treatments. The risk register, risk profile, and progress against treatments should also be monitored and reviewed.

### Tips and traps

You should identify the range or type of events that may result in a review of the risk assessment. A review of the risk assessment must include consideration of new or unidentified risks as well as the effectiveness of any new treatments or controls put in place.

## Communication and consultation

### Why is this important?

Risk management cannot be done in isolation. Engaging with relevant stakeholders is essential throughout the risk management process. It is also important to communicate and consult with anybody who may be affected by the risk, its controls or treatments.

Communication, consultation, sharing and receiving information with external and internal stakeholders should take place during all stages of the risk management process.

A consultative approach will:

- help establish the context appropriately
- ensure that the interests of stakeholders are understood and considered
- help ensure that risks are adequately identified
- bring different areas of expertise together for analysing risks
- ensure that different views are appropriately considered when defining risk criteria and in evaluating risks
- secure endorsement and support for a treatment plan
- enhance appropriate change management during the risk management process.

### Minimum requirements

Ensure that all relevant stakeholders are involved in the risk management process

Ensure those responsible for implementing actions understand the basis of how decisions have been made and what specifically is required by them.

### Tips and traps

Stakeholders can be essential in helping you identify risks and treatment strategies. There are generally four types of stakeholders:

- Those who are directly impacted by the risk
- Those who may impact the risk
- Those who are managing controls for the risks
- Risk management areas (i.e. areas in charge of setting policy direction for risk management).

## Recording and reporting risks

Comcare has created risk register templates to formalise the capture and monitoring of all identified risks. These can be found on the risk management [ComNet page](#). The results of the risk management process must be documented in a risk register. Existing risk registers include:

- Strategic risk register: For recording whole-of-Comcare strategic risks defined by the CEO and Executive Committee.
- Group risk register: For recording risks identified by each Group's Executive.
- Operational/project risk registers: For recording risks specific to a team or project.
- Fraud and corruption risk register: For recording fraud and corruption risks.

Comcare will actively report to internal and external stakeholders about risk and risk management. Reporting mechanisms include, but are not limited to:

- quarterly reporting of strategic risk register progress to the Executive Committee and the Audit and Risk Committee
- Regulator Performance Framework reports
- external audits comprising risk as an element
- regular reporting at the Group level on Group risk registers (at least biannually).

## Appendix 1 - Comcare risk assessment criteria

Control Effectiveness			
Rating	Descriptor	Design effectiveness	Implementation effectiveness
Effective	Existing controls address risk, are in operation and are applied consistently. Management is confident that the controls are effective and reliable. Ongoing monitoring required.	Y	Y
Requires assurance	Management needs further information on the effectiveness of the controls as: there has not been enough monitoring and review activities to inform a judgement it is a new control	?	?
Room for improvement	Controls are only partially effective, require ongoing monitoring and may require it be redesigned, improved or supplemented.	Y	N
		N	Y
Ineffective	Management cannot be confident that any degree of risk modification is being achieved. Controls need to be redesigned.	N	N

Table 3: Control Effectiveness

Consequence					
	Insignificant	Minor	Moderate	Major	Severe
Business Objectives	Objectives almost certainly will be achieved	Objectives likely to be achieved despite impact	Require resourcing adjustment to achieve objectives	Would threaten achievement of objectives	Would stop achievement of objectives
Operational	Business interruption < 1 day Financial loss of less than 1% of project or activity value	Business interruption up to 1 day Financial loss of 1-5% of project or activity value	Business interruption 1 to <2 days Financial loss of 5-15% of project or activity value	Business interruption 2 to 5 days Financial loss of 15-30% of project or activity value	Business interruption > 5 days Financial loss more than 30% project or activity value
Reputation	Minor internal dissatisfaction	Complaint from key stakeholder or some internal displeasure	Localised public and media headlines	High level political, public and national media criticism	Intense political, public and national media criticism Government Intervention

<b>People Safety</b>	No medical treatment required	First aid only	Less serious injury requiring medical treatment	Serious injuries requiring hospital treatment	Fatalities or critical injuries
<b>Property</b>	No damage to equipment	Minor damage to non-essential equipment	Damage to property or essential equipment	Major damage to essential property, equipment or environment	Severe damage to essential property, equipment or environment
<b>Data Security</b>	No data corruption or unintended disclosures	Confidential Comcare data disclosed internally beyond need to know	Minor privacy breach or data corruption	Critical data leak, tampering or inaccessible for more than 5 days	Critical data destroyed or significant privacy breach
<b>Project Management</b>	See <a href="#">Program and Project Management Framework, Appendix 3, p29</a>	See <a href="#">Program and Project Management Framework, Appendix 3, p29</a>	See <a href="#">Program and Project Management Framework, Appendix 3, p29</a>	See <a href="#">Program and Project Management Framework, Appendix 3, p29</a>	See <a href="#">Program and Project Management Framework, Appendix 3, p29</a>
<b>Investment versus Liability Loss</b>	See Premium Framework and Investment Policy	See Premium Framework and Investment Policy	See Premium Framework and Investment Policy	See Premium Framework and Investment Policy	See Premium Framework and Investment Policy

Table 4: Risk Consequence

Likelihood	
<b>Almost Certain</b>	Expected in most circumstances
<b>Likely</b>	Will probably occur in most circumstances
<b>Possible</b>	Could occur at some time
<b>Unlikely</b>	Not expected to occur
<b>Rare</b>	Exceptional circumstances only

Table 5: Risk likelihood



Risk Rating Matrix					
	Consequence				
Likelihood	Insignificant	Minor	Moderate	Major	Severe
Almost Certain	Low acceptable	Medium acceptable	High unacceptable	Extreme unacceptable	Extreme unacceptable
Likely	Low acceptable	Medium acceptable	High unacceptable	Extreme unacceptable	Extreme unacceptable
Possible	Low acceptable	Medium acceptable	Medium acceptable	High unacceptable	Extreme unacceptable
Unlikely	Low acceptable	Low acceptable	Medium acceptable	Medium acceptable	High unacceptable
Rare	Low acceptable	Low acceptable	Low acceptable	Medium acceptable	Medium acceptable

Table 6: Risk Rating Matrix

Current Risk Level	Risk Escalation/Mitigation Level	Monitoring Regime
Extreme	The CEO and Executive Committee must be informed to decide whether to accept or otherwise mitigate material risk.	Monthly reporting to Executive Committee
High	Responsible General Manager to determine appropriate mitigation and assign responsibility.	Quarterly reporting to appropriate operational area and Authoritative Committee
Medium	Manage by appropriate internal controls and regular monitoring.	Reviewed quarterly, as appropriate
Low	Unlikely to need specific application of resources.	Reviewed annually, as appropriate

Table 7: Risk escalation, mitigation and monitoring

## Appendix 2 - Risk tools

This attachment provides additional information on some of the tools and techniques that are described in Step 1: Risk Identification.

### The Butterfly or Bowtie

The risk butterfly technique or bowtie helps you map out different levels of causes and consequences.

At its simplest level, it looks like:



Figure 6: Risk Bowtie

However, you can then use the risk bowtie to think about second order causes and consequences.

### Fishbone (Cause and Effect or Ishikawa) Diagrams

The fishbone diagram identifies many possible causes for risk. It can be used to structure a brainstorming session. It sorts ideas into useful categories.

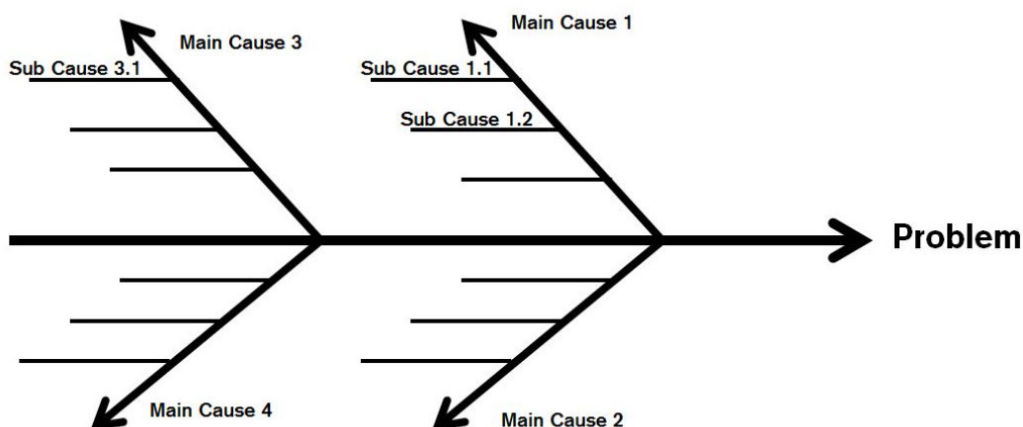


Figure 7: Fishbone Diagram

## ATTACHMENT B - Comcare risk registers and reporting

Development and ownership	Reporting and documentation
<b>STRATEGIC RISK REGISTER</b>	
<ul style="list-style-type: none"> <li>Details Comcare's strategic risks</li> <li>Focusses on risks with broad organisational impact</li> <li>CEO, with the Executive Committee, defines strategic risks when they arise and at least annually</li> <li>Risks are based on pre-defined focus areas, against Comcare's strategic priorities</li> <li>Members of the Executive Committee own strategic risks</li> </ul>	<ul style="list-style-type: none"> <li>Documented in the Strategic Risk Register</li> <li>Risks reported quarterly to Executive and Audit Committees</li> <li>Chief Operating Officer is responsible for reporting on strategic risks</li> <li>GM Legal is responsible GM for reporting on emerging risks. Emerging strategic risks must be identified, assessed, evaluated, treated (as appropriate), recorded in the relevant risk register, and included in future reporting.</li> </ul>
<b>OPERATIONAL/PROJECT RISK REGISTER</b>	
<ul style="list-style-type: none"> <li>Details risks of a specific Comcare wide compliance requirement (eg Fraud Control, Protective Security, Child Safety, WHS) work area or project</li> <li>Operational risks are at least identified annually or when circumstances require. Project risks are defined during the project planning stage.</li> <li>The risk owner for each operational/project risk is a senior employee/project manager</li> <li>Risks may be mapped to Group risks and strategic risks.</li> </ul>	<ul style="list-style-type: none"> <li>Operational/project risks are documented in the relevant Operational specific / or project risk register</li> <li>Risks to be reported to relevant Operations or Performance Compliance and Engagement Committee, Portfolio Management Board Meeting/Project Committee</li> <li>Specific risks raised to the Group Executive Meeting as appropriate</li> <li>The Director/Project Manager is responsible for the reporting on operational/project risks</li> <li>Emerging operational/project risks must be identified, assessed, evaluated, treated (as appropriate), recorded in the relevant risk register, and included in future reporting.</li> </ul>
<b>GROUP RISK REGISTER</b>	
<ul style="list-style-type: none"> <li>Details Group risks</li> <li>Focusses on risks with a broad Group impact</li> <li>The General Manager/s will identify Group risks annually</li> <li>The risk owner for each Group risk is a member of Group's senior management.</li> <li>Risks are based on pre-defined focus areas and must map to the relevant strategic priorities.</li> </ul>	<ul style="list-style-type: none"> <li>Documented in the relevant Group's risk register</li> <li>Risks to be reported biannually to the Chief Operating Officer and CEO.</li> <li>The General Managers are responsible for reporting on Group risks and escalating high and extreme risks through the appropriate operational area and Authoritative Committee</li> <li>Emerging group risks must be identified, assessed, evaluated, treated (as appropriate), recorded in the relevant risk register, and included in future reporting.</li> </ul>

Guidance on how to identify and assess the above categories of risk is contained within the relevant register templates.



## Operations Committee Reporting

The responsibility for coordinating cross group input and reporting arrangements, including the frequency of reporting to the Operations Committee are listed in the table below:

Operational Risk Area	Responsible Executive	Responsible Team	Frequency of Reporting
Fraud Control	Chief Operating Officer	Finance and Assurance	Biannual
Protective Security	Chief Operating Officer	People, Property and Security in conjunction with Technology and Information Management	Annual
Work Health and Safety <sup>3</sup>	Chief Operating Officer	People, Property and Security	Annual
Child Safety	Chief Operating Officer	Finance and Assurance	Annual
Modern Slavery	Chief Operating Officer	Finance and Assurance	Annual

*Table 8: Operations Committee risk reporting*

---

<sup>3</sup> WHS risks are reported to the National Health and Safety Committee (NHSC). The NHSC monitors Comcare's WHS performance and reports on progress to the Operations Committee.

## ATTACHMENT C - Risk appetite and tolerance

Risk appetite is the amount of risk Comcare is willing to accept or retain in order to achieve our objectives. Risk tolerance represents the practical application of risk appetite. Comcare will not tolerate risks which could expose it to:


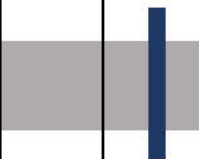
- unacceptable levels of financial loss relative to programme and project administration
- significant delays to programme or project delivery
- inconsistency in regulatory decisions
- breaches of legislative or regulatory obligations through illegal or negligent actions
- unsatisfactory impact to employee's health, welfare and safety.

Comcare recognises that many of its activities have residual risk and that it is not possible or necessarily desirable to eliminate all risk. Comcare will accept risk providing that the activity is:

- consistent with Comcare's objectives
- a proper use of public resources for which Comcare is responsible
- subject to appropriate performance and conformance measures
- supportive of Comcare's approach to innovation and provides an opportunity to test and learn
- a high priority proactive regulatory activity.

Comcare's risk appetite and tolerance by risk category are described in the following table:

Appetite is shown by the navy line. Tolerance is shown by the grey block. The levels align with the Comcare Risk matrix, noting that extreme is excluded as it is not considered a tolerable level. The terms 'very low' and 'not tolerate' are used to reinforce these risks are to be reduced as much as practical. Comcare is committed to remedial action where risk eventuates.

Risk category	Appetite / Tolerance level			Appetite / Tolerance statement
	Low	Mod	High	
Finances				Comcare is committed to managing public resources efficiently, effectively, economically and ethically. We have a <b>very low risk appetite</b> related to financial management. We have a <b>very low tolerance</b> for systemic control failures or breakdowns and unexplained variances to administered finances.
Program/project, service design				Comcare is committed to delivering high quality business outcomes and we aim to improve outcomes through ongoing monitoring of performance and evaluation. Comcare has a <b>moderate risk appetite</b> in the pursuit of innovation to achieve business outcomes, where reasonable steps have been taken to implement effective governance arrangements.

Service delivery				Comcare is committed to delivering high quality service delivery outcomes to our stakeholders and we aim to improve outcomes through ongoing monitoring of performance and evaluation. We have a <b>low tolerance</b> for non-delivery and expect that delivery risks will be identified, managed and, where needed, escalated to ensure appropriate visibility.
Regulatory decisions				Comcare is committed to maintaining effective and efficient regulatory frameworks that are fit for purpose, proportionate to risk, and continuous improvement. We have a <b>low risk appetite</b> for regulatory risks and we have a <b>low tolerance</b> for inconsistency in regulatory decisions and/or compliance with regulatory obligations.
Legal and Compliance				Comcare is committed to compliance with relevant legislation, regulation, best practice as well as internal policies and governance requirements. We have a <b>low risk appetite</b> for non-compliance where we have taken all reasonable steps to understand the legislative environment that we operate in. We will <b>not tolerate</b> deliberate or purposeful violations of legislative or regulatory requirements.
Privacy				Comcare is committed to protecting all personal and sensitive information. We have a <b>very low risk appetite</b> relating to breaches of privacy. The risk may only be accepted where all legislative privacy control requirements are in place and the risk has been reduced to the point where additional controls have negative cost/benefit. We will <b>not tolerate</b> any deliberate action that would constitute an interference with an individuals' privacy, or otherwise be inconsistent with Comcare's privacy obligations.
Integrity, Fraud and Corruption				Comcare recognises that there is a risk of fraud and corruption within our activities. We have a <b>very low appetite</b> for unethical behaviour and we will <b>not tolerate</b> fraud or corruption. We will take all reasonable steps to prevent, detect and respond to fraud, corruption and failings in integrity.
Work Health and Safety				Comcare is committed to providing safe work for all workers (including employees and contractors) and visitors that is free from physical or psychological harm. There is a <b>very low appetite</b> for the potential of injuries of employees and contractors, recognising that there is inherent risk in some work practices and locations.
Government expectations				Comcare is committed to upholding our reputation and providing professional, impartial and reliable advice and support to our Ministers and their offices. There is a <b>low risk appetite</b> for risks that impede the implementation of key Government initiatives or damage productive government relationships. We have a <b>low tolerance</b> for behaviour that could damage these relationships or our reputation resulting from poor advice or support or as a scheme authority.
Stakeholders				Our relationships with stakeholders supports our policy development and helps us to achieve our purposes and objectives. Open discussions are critical to designing our policy and regulatory approaches. It is



			important we understand the different perspectives of our stakeholders, even where we do not agree. We have a <b>moderate risk appetite</b> for reputational damage arising from policy differences where we have engaged openly and robustly in a professional manner. We have a <b>low tolerance</b> for policy and regulatory approaches that are designed without meaningful stakeholder engagement.
Information, Systems and security			Comcare invests in processes, systems and technology that are fit for purpose and enable Comcare to achieve its purposes and objectives in an effective and efficient manner. We have a <b>low risk appetite</b> related to security risks, information management processes and systems to support business requirements. We take a strong, risk-managed approach to security that matches the threat environment for both physical and information security. There is a <b>moderate tolerance</b> associated with manual systems and outage of non-critical internal systems, accepting that some inefficiency may exist, and non-critical errors may occur, provided they do not result in a breach of legislation, regulation, privacy and/or result in litigation. We have a <b>very low tolerance</b> for practices that result in critical business failure, misuse of our systems, encourage loss or unauthorised disclosure of sensitive information, or system unavailability beyond the agreed disaster recovery/business continuity recovery times.
Policy development and advice			Comcare engages with risk to take innovative approaches to developing policy. We take risks commensurate with the complexity and uncertainty of the problem. We develop policy and provide advice based on evidence, data and research. We have a <b>moderate risk appetite</b> related to identifying, proposing and deploying innovative approaches or new ideas that support the achievement of our purposes, where we have appropriately scoped issues, engaged with key internal and external stakeholders and adequately considered the associated risks and benefits. We have a <b>very low tolerance</b> for advice that is inaccurate, misleading or in any way undermines Comcare's reputation for providing reliable and high-quality advice.
Workforce			Comcare is committed to building a capable, professional and responsive workforce which enables Comcare to deliver on its priorities. We have a <b>moderate risk appetite</b> for risks to Comcare's skills, knowledge and expertise and will continue to proactively invest in our people. We have a <b>low tolerance</b> for ongoing staff underperformance.

- NB- This table is for guidance and where instances of risk occur that may not align, please discuss with your manager/executive.

## ATTACHMENT D - Risk capabilities

### APSC Work Level Standards

Competencies		Required training
EL2	Identify, manage and evaluate risk in all decision making and delivery of outcomes	<ul style="list-style-type: none"> <li>• Face-to-face risk management workshops</li> <li>• Corporate Fundamentals: Risk Essentials</li> <li>• Corporate Fundamentals: Fraud Essentials</li> </ul>
EL1	Engage with risk, including the conduct of risk assessment and risk management activities for area of responsibility	<ul style="list-style-type: none"> <li>• Face-to-face risk management workshops</li> <li>• Corporate Fundamentals: Risk Essentials</li> <li>• Corporate Fundamentals: Fraud Essentials</li> </ul>
APS6	Evaluate the effectiveness of risk management and risk assessment activities within sphere of responsibility	<ul style="list-style-type: none"> <li>• Face-to-face risk management workshops</li> <li>• Corporate Fundamentals: Risk Essentials</li> <li>• Corporate Fundamentals: Fraud Essentials</li> </ul>
APS5	Assist with audits and maintaining appropriate risk management programs	<ul style="list-style-type: none"> <li>• Corporate Fundamentals: Risk Essentials</li> <li>• Corporate Fundamentals: Fraud Essentials</li> </ul>
APS4	Identify and mitigate risks that will impact on own and teamwork outcomes	<ul style="list-style-type: none"> <li>• Corporate Fundamentals: Risk Essentials</li> <li>• Corporate Fundamentals: Fraud Essentials</li> </ul>
APS3	Identify, gather, record and share information for risk analysis activities, and development of compliance strategies	<ul style="list-style-type: none"> <li>• Corporate Fundamentals: Risk Essentials</li> <li>• Corporate Fundamentals: Fraud Essentials</li> </ul>
APS2	Identify and actively manage risks that will affect day-to-day work	<ul style="list-style-type: none"> <li>• Corporate Fundamentals: Fundamentals of Risk Management</li> <li>• Corporate Fundamentals: Fraud Awareness</li> </ul>



## ATTACHMENT E – Shared risk

### What is a shared risk?

The Commonwealth Risk Management Policy defines shared risk as:

*‘Risks extending beyond a single entity which require shared oversight and management’.*

Commonwealth entities are required to establish arrangements to understand and contribute to the management of shared risks.

### Types of risk Comcare shares

Comcare has responsibility for managing shared risk as part of our core business. For example: through insurance, employers share the risk of significant financial loss with Comcare. Through our regulator role, we share the risk of promoting and enabling safe and healthy workplaces with employers.

An overview of the types of risk Comcare shares is outlined in Table 8.

Types of shared risk	Examples
Risk is shared because two or more organisations that want to achieve the same objective. This objective may be explicit or implied, and the entities share the risk due to their situation or legal obligation (i.e. there is no formal partnership or contract).	<ul style="list-style-type: none"> <li>Both Comcare and employers have responsibility for achieving the objective of a healthy and safe workplace. A risk to this objective would be that employees do not advise Comcare of all notifiable instances. The employer would have responsibility for ensuring that appropriate policies and processes are set up and communicated with their employees. However, the risk is partially shared with Comcare, given our role in scheme design and regulation. To reduce this risk, Comcare and the employer would be expected to work together.</li> <li>Each Comcare office has shared resilience risks with other nearby organisations, such as fire, power outage or road closures.</li> </ul>
Risk is shared through a formal partnership to achieve specific objectives.	<ul style="list-style-type: none"> <li>Comcare shares risks with public, private and not-for-profit organisations through the Collaborative Partnership Programme. All parties have a role to play in the partnership, therefore they share the risk that it does not achieve its intended outcomes.</li> <li>Research partnerships - Comcare is responsible for prioritising research themes and managing our research partners. Our research partners are responsible for ensuring the research is conducted effectively. As a result, Comcare and our partners share the risk of achieving the best evidence-based information to inform our strategic priorities.</li> </ul>

Risk is shared through contractual arrangements.	<ul style="list-style-type: none"> <li>▶ The risk of ineffective providers would impact Comcare, individual employers, and claimants, although the impact on each party differs. Each party has a different amount of control over this risk, depending on who has engaged the specific providers.</li> <li>▶ The risk of unsuccessful delivery of services by a supplier, such as an unsuccessful technical rollout of an ICT system. In this instance, Comcare would be accountable for the overall outcome; however, both Comcare and the supplier would be responsible for implementing relevant controls.</li> </ul>
--	---

Table 9: Types of risk Comcare shares with other entities

## Principles for managing shared risk

When managing shared risks with other entities, Comcare employees should adopt the following principles:

- Not undertaken separately from other risk management. Wherever possible, the management of shared risk should be undertaken through existing risk management processes. Any risk plans or risk registers developed to manage shared risks should not duplicate existing risk documentation.
- Focus on achieving objectives, not just on documentation. The purpose of documenting a risk assessment is to ensure appropriate visibility and oversight of our risks, and to ensure a consistent approach is applied. By keeping the objective in mind, risk is linked to planning and decision making rather than being a compliance or 'tick the box' exercise.
- Tailored approach and understanding what is within our control. The approach taken to managing shared risks with a service provider would need to be different to managing shared risks for delegated claims. The key principle to keep in mind is to consider what we can control, and what is outside our control. Managing shared risk effectively is about identifying controls that are our responsibility and identifying where we need to monitor and manage external parties to reasonably ensure they are implementing the controls that they are responsible for.

## Steps for effectively managing shared risks

When considering and documenting shared risks, the following steps may assist:

- Determine who is responsible for the outcome. Identifying the parties involved in a project or activity will help determine whether there are any shared risks. Consider the roles of each stakeholder, what responsibility they have, and who is ultimately accountable for the outcome. Once identified, consider what control they have over the risk and what part they play.
- Consider responsibility versus accountability. Often the concept of shared risk is overlooked, particularly in contractual situations, where the risk is seen to be 'outsourced'. An example of this is writing into a contract that a contracted provider must comply with WHS law. If the provider has an incident, and a member of the public is harmed, the liability could be shared between the provider and the agency who funded the activity (Comcare). While we can't control their actions, we should take reasonable steps to ensure that they are following the terms of the agreement, such as conducting due diligence and assurance over the contract.

- Include a discussion on shared risk as part of each meeting, using the risk register to focus discussion. Where parties that share risk are meeting on a joint project or activity, it may be useful to focus each meeting on risk and include targeted questions on what needs to be improved.
- Embed risk sharing mechanisms in contracts. For example, establish an 'at risk' component of the contract where the supplier could gain or lose revenue based on achieving Key Performance Indicators. Oversight and assurance of service provision is another method, as is thorough due diligence to verify the past performance of a supplier.



## Risk Appetite and Tolerance Statement<sup>1</sup>

### Risk Appetite and Tolerance

Risk appetite is the amount of risk Comcare is willing to accept or retain in order to achieve our objectives. Risk tolerance represents the practical application of risk appetite. Comcare will not tolerate risks which could expose it to:



- unacceptable levels of financial loss relative to programme and project administration
- significant delays to programme or project delivery
- inconsistency in regulatory decisions
- breaches of legislative or regulatory obligations through illegal or negligent actions
- unsatisfactory impact to employee's health, welfare and safety.

Comcare recognises that many of its activities have residual risk and that it is not possible or necessarily desirable to eliminate all risk. Comcare will accept risk providing that the activity is:

- consistent with Comcare's objectives
- a proper use of public resources for which Comcare is responsible
- subject to appropriate performance and conformance measures
- supportive of Comcare's approach to innovation and provides an opportunity to test and learn
- a high priority proactive regulatory activity.

Comcare's risk appetite and tolerance by risk category are described in the following table:

Appetite is shown by the navy line. Tolerance is shown by the grey block. The levels align with the Comcare Risk matrix, noting that extreme is excluded as it is not considered a tolerable level. The terms 'very low' and 'not tolerate' are used to reinforce these risks are to be reduced as much as practical. Comcare is committed to remedial action where risk eventuates.

Risk category	Appetite / Tolerance level			Appetite / Tolerance statement
	Low	Mod	High	
Finances				Comcare is committed to managing public resources efficiently, effectively, economically and ethically. We have a <b>very low risk appetite</b> related to financial management. We have a <b>very low tolerance</b> for systemic control failures or breakdowns and unexplained variances to administered finances.
Program/project, service design				Comcare is committed to delivering high quality business outcomes and we aim to improve outcomes through ongoing monitoring of performance and evaluation. Comcare has a <b>moderate risk appetite</b> in the pursuit of innovation to achieve business outcomes, where reasonable steps have been taken to implement effective governance arrangements.

Risk category	Appetite / Tolerance level			Appetite / Tolerance statement
	Low	Mod	High	
Service delivery				Comcare is committed to delivering high quality service delivery outcomes to our stakeholders and we aim to improve outcomes through ongoing monitoring of performance and evaluation. We have a <b>low tolerance</b> for non-delivery and expect that delivery risks will be identified, managed and, where needed, escalated to ensure appropriate visibility.
Regulatory decisions				Comcare is committed to maintaining effective and efficient regulatory frameworks that are fit for purpose, proportionate to risk, and continuous improvement. We have a <b>low risk appetite</b> for regulatory risks and we have a <b>low tolerance</b> for inconsistency in regulatory decisions and/or compliance with regulatory obligations.
Legal and Compliance				Comcare is committed to compliance with relevant legislation, regulation, best practice as well as internal policies and governance requirements. We have a <b>low risk appetite</b> for non-compliance where we have taken all reasonable steps to understand the legislative environment that we operate in. We will <b>not tolerate</b> deliberate or purposeful violations of legislative or regulatory requirements.
Privacy				Comcare is committed to protecting all personal and sensitive information. We have a <b>very low risk appetite</b> relating to breaches of privacy. The risk may only be accepted where all legislative privacy control requirements are in place and the risk has been reduced to the point where additional controls have negative cost/benefit. We will <b>not tolerate</b> any deliberate action that would constitute an interference with an individuals' privacy, or otherwise be inconsistent with Comcare's privacy obligations.
Integrity, Fraud and Corruption				Comcare recognises that there is a risk of fraud and corruption within our activities. We have a <b>very low appetite</b> for unethical behaviour and we will <b>not tolerate</b> fraud or corruption. We will take all reasonable steps to prevent, detect and respond to fraud, corruption and failings in integrity.
Work Health and Safety				Comcare is committed to providing safe work for all workers (including employees and contractors) and visitors that is free from physical or psychological harm. There is a <b>very low appetite</b> for the potential of injuries of employees and contractors, recognising that there is inherent risk in some work practices and locations.
Government expectations				Comcare is committed to upholding our reputation and providing professional, impartial and reliable advice and support to our Ministers and their offices. There is a <b>low risk appetite</b> for risks that impede the implementation of key Government initiatives or damage productive government relationships. We have a <b>low tolerance</b> for behaviour that could damage these relationships or our reputation resulting from poor advice or support or as a scheme authority.
Stakeholders				Our relationships with stakeholders supports our policy development and helps us to achieve our purposes and objectives. Open discussions are



Risk category	Appetite / Tolerance level			Appetite / Tolerance statement
	Low	Mod	High	
				critical to designing our policy and regulatory approaches. It is important we understand the different perspectives of our stakeholders, even where we do not agree. We have a <b>moderate risk appetite</b> for reputational damage arising from policy differences where we have engaged openly and robustly in a professional manner. We have a <b>low tolerance</b> for policy and regulatory approaches that are designed without meaningful stakeholder engagement.
Information, Systems and security				Comcare invests in processes, systems and technology that are fit for purpose and enable Comcare to achieve its purposes and objectives in an effective and efficient manner. We have a <b>low risk appetite</b> related to security risks, information management processes and systems to support business requirements. We take a strong, risk-managed approach to security that matches the threat environment for both physical and information security. There is a <b>moderate tolerance</b> associated with manual systems and outage of non-critical internal systems, accepting that some inefficiency may exist, and non-critical errors may occur, provided they do not result in a breach of legislation, regulation, privacy and/or result in litigation. We have a <b>very low tolerance</b> for practices that result in critical business failure, misuse of our systems, encourage loss or unauthorised disclosure of sensitive information, or system unavailability beyond the agreed disaster recovery/business continuity recovery times.
Policy development and advice				Comcare engages with risk to take innovative approaches to developing policy. We take risks commensurate with the complexity and uncertainty of the problem. We develop policy and provide advice based on evidence, data and research. We have a <b>moderate risk appetite</b> related to identifying, proposing and deploying innovative approaches or new ideas that support the achievement of our purposes, where we have appropriately scoped issues, engaged with key internal and external stakeholders and adequately considered the associated risks and benefits. We have a <b>very low tolerance</b> for advice that is inaccurate, misleading or in any way undermines Comcare's reputation for providing reliable and high-quality advice.
Workforce				Comcare is committed to building a capable, professional and responsive workforce which enables Comcare to deliver on its priorities. We have a <b>moderate risk appetite</b> for risks to Comcare's skills, knowledge and expertise and will continue to proactively invest in our people. We have a <b>low tolerance</b> for ongoing staff underperformance.

NB- This table is for guidance and where instances of risk occur that may not align, please discuss with your manager/executive.

<sup>i</sup> This Statement is an extract from the Risk Management Procedure, Attachment D.

Comcare Emerging Risk Process

Purpose

The purpose of the Comcare Emerging Risks process is to identify new risks manifesting within Comcare’s operating environment that require management.

Emerging risks are newly developing or evolving risks that can affect the achievement of an organisation’s objectives. These risks present Comcare with newfound challenges and difficulties, of which the consequences are currently unknown. Emerging risks can materialise quickly and unexpectedly and often have complex consequences and characteristics that make them difficult to manage. This uncertainty can be hard to anticipate and even more difficult to measure.

This process support’s Comcare in meeting the requirements of the [Commonwealth Risk Management Policy](#) to have arrangements for identifying, managing and escalating emerging risks as shown in Figure 1. Emerging risk process.

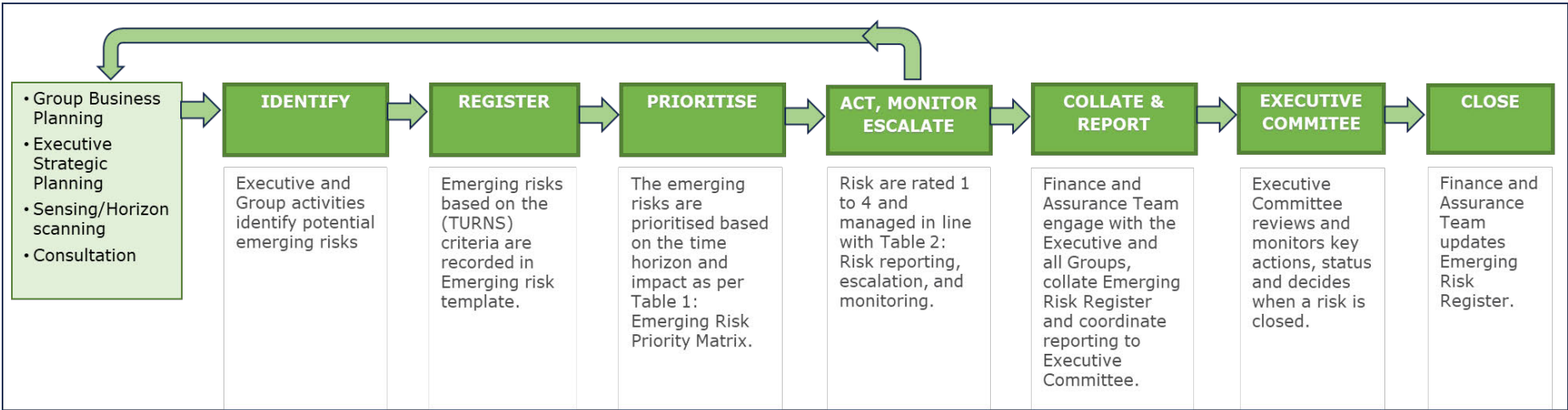


Figure 1. Emerging risk process

Process

Identification

Emerging risks can be conditions, situations or trends that may be observed in the wider community or internally. They may be complex in nature and can be rapidly changing or evolving. Due to the inherent level of uncertainty associated with emerging risks, they can be hard to anticipate and even more difficult to measure. They should be supported by indications and reasonable information that justifies the emerging risks as being material and needing further assessment.

All Groups will be asked by the Finance and Assurance Team<sup>1</sup> on a regular<sup>2</sup> basis to identify items for considerations based on the Emerging Risk criteria (acronym TURNS) as follows:

- **Timing** - the risk would materialise beyond the immediate strategic risk horizon, 6 months to multiple years out.
- **Uncertainty** - there is a greater degree of uncertainty associated with the risk as not all facts are known or measurable
- **Relevance** - The risk must directly relate to Comcare
- **Novelty** - it is not a risk previously considered or expected
- **Source** - change and disruption in the external environment creates new sources of risk not previously considered

There are a number of mechanisms that can be used in order to identify emerging risks: risk sensing, strategic and business planning and consultation.

- **Risk Sensing:** Groups are encouraged to examine all of the information and data available to detect any early indicators of an emerging risk in their operating environment. This is also known as horizon scanning and works towards enhancing situational awareness and understanding of the internal and external operating environments. Media reports, research, external publications, global and localised trend data are useful with gaining intelligence on emerging risks. Some of the methodologies involved in risk sensing include:
  - **SWOT analysis:** This is a methodical examination of Strengths, Weaknesses, Opportunities and Threats. It is a useful approach for identifying any external or internal trends and factors that give rise to risk.
  - **PESTLEE analysis:** This stands for Political, Economic, Social, Technological, Environmental and Ethical. This provides a useful framework to guide thinking in identifying risks that are on the horizon, by providing consistent categories to consider these risks. This analysis should enable entities to understand the events that could occur or are occurring in their external context that can make a difference to an entity’s ability to carry out functions and activities and reach strategic outcomes.
- **Strategy and Business planning:** Risk sensing intelligence may also be one of the inputs to Executive and Group planning sessions. Emerging risk is an essential part of the discussion for any strategic or group level planning and risk analysis. It is incorporated into these activities as normal process. This is important because when identifying our goals we must also be considering the future dependencies or uncertainties that could stand in the way of achieving these objectives. Through reviewing our corporate plan, group plans, risk registers and identifying drivers of success, we may be able to identify more clearly what must go right if you are to achieve these objectives and consider any potential roadblocks and barriers that may prevent the fulfilment of these objectives.
- **Consultation:** This may occur with both internal and external stakeholders that facilitate a discussion and awareness about any potential emerging risks. This may be focused through risk-based workshops, planning meetings or come about through forum discussions or feedback and complaint mechanisms. Leveraging insights or recommendations from the Executive Committee or other authoritative bodies such as the Commissions and the Audit and Risk Committee also provide opportunities to identify emerging risk.

<sup>1</sup> Coordinated by the Assistant Director Risk Management and Fraud Control

<sup>2</sup> Regular basis means at least three times annually, including the annual Executive Strategic planning session and Group planning sessions. Additional reporting and escalation will occur according to priority and status changes as noted in Table 2.



### Management

Once the Executive and Groups have conducted their risk identification, it is important to turn the risk signals and intelligence into strategic insights to inform decision-making.

#### Emerging Risk register

After identifying emerging risks, the next step is for the Groups to record this information in a register. The Finance and Assurance Team will provide all Groups with the relevant Emerging Risk Register template as shown in Table 3. For completion of the register, Groups will need to consider the following:

- **ID** - unique identifier
- **Date Added (Year/Month)** – Insert the date when the risk first entered on the register.
- **Emerging Risk**- Provide a short title.
- **Lead Group responsible** - indicate the lead Group responsible, using abbreviations provided.
- **Source** - What is the main cause of the risk? Select one of the following sources:
  - Bills/Policy Initiatives
  - Legislative amendments
  - Parliamentary Inquiries
  - Reforms
  - Changes in Government or policy agenda
  - External Reviews
  - Social
  - Economic
  - Technological
  - Other & Source (i.e Licensee insolvency) Please provide the source.
- **Description** - Provide a description of the emerging risk, including how it has arisen, the relevant stakeholders and how it affects Comcare. Also is the risk a potential threat or opportunity or provides both types?
- **Strategic Risk Focus Area** – Select the most applicable area: Capability, Governance, Culture, Stakeholders
- **Strategic Priority** - As listed in our current Corporate Plan, which strategic priority/s does the emerging risk impact?
- **Time Horizon** - How long until the emerging risk could first be realised at Comcare? Select the time frame.
- **Impact** - What is the best estimate of the potential consequence to Comcare of the emerging risk at this point in time? Select the impact level.
- **Priority** - This is rated using Comcare's Priority Matrix (see below). This is based on the intersection of the assessment of the Time horizon and the Impact.
- **Action (Responsibility/Due date)** - List all actions Comcare will undertake to prepare for manage the emerging risk, including responsibility and due date. This may include what triggers, warnings or key risk indicators (detective controls) are being actively monitored to understand the emergence or evolution of the risk.

An example of a completed entry is provided in Table 4.

#### Priority

The emerging risk will be rated based on assessment of the Time Horizon and Impact of the emerging risk as shown in Table 1. Emerging risk priority matrix.

The Time Horizon is a measure of the anticipated time for the risk to significantly impact Comcare. As shown in the Table 1 below this is considered against three time frames:

- **Short-term** - within 3 to 6 months
- **Mid-term** - within 6 to 12 months
- **Long-term** - over 12 months

Impact is the measure of the effect of the emerging risk on Comcare's key priorities and operations. As shown in Table 1 below this is considered against three impact levels:

- **High** -serious impact to threaten key priorities and operations; major political, public and national media criticism; additional large increase in budget is required as well as additional resourcing, policy and education; major damage to systems, data, assets and injury of people.
- **Moderate** - moderate impact to key priorities and operations; localised public and media headlines; small adjustments to budgetary position, resourcing, policy and education; some damage to systems, data, assets and injury of people, well above just BAU activities/controls required.
- **Low** - minimal disruption or changes to key priorities, objectives, budget and operations; minimal damage to systems, data, assets or injury of people, can manage with BAU activities/controls or minor changes.

The priority is a four-score scale of 1 to 4. A rating of 1 is the highest priority with 4 as the lowest.

PRIORITY MATRIX		Impact		
		High	Moderate	Low
Time Horizon	Short-term within 3 to 6 months	1	2	3
	Mid-term within 6 to 12 months	1	2	3
	Long-term over 12 months	2	3	4

Table 1. Emerging risk priority matrix



All potential emerging risks must be approved by the raising group's General Manager and the templates returned to the Finance and Assurance Team for collation and quality assurance. The Finance and Assurance Team will prepare and submit the emerging risk register and report to the EC. The COO will present the report to the EC.

#### *Monitoring and Reporting*

Groups will be asked to provide updates on the emerging risks they identify and own. All Groups will maintain one point of contact for coordination of identification and reporting to the Finance and Assurance team as listed in Table 7 below. Requests will occur at least three times annually, including the preparations for the annual Executive Strategic planning session and Group planning sessions. The schedule will be dependent upon the timings of these planning sessions and Executive Committee meetings (for reporting) and Audit and Risk Committee dates (to allow input from these meetings). Additional reporting and escalation will occur according to priority and status changes as noted in Table 2. Risk reporting, escalation, and monitoring. The updates should address any changes in the background to the risk together with accountabilities and responsibilities for active monitoring, actions undertaken by Comcare to manage it if the level of priority has changed as indicated in Table 2. For Priority 1 and 2 emerging risks, oversight is required at Executive Committee level either due to the priority or the action requiring input and collaboration across Comcare.

Current Priority	Reporting and Escalation	Monitoring Regime
1	The CEO and Executive Committee (EC) must be informed on how this risk is being actively managed via scheduled reporting or advised sooner if scheduled reporting is greater than in a month's time. Accountabilities and responsibilities to be allocated and oversighted by the EC. GM to escalate immediately by exception reporting to EC if oversight input on the management of the risk is required.	Active monitoring to seek greater clarity on the consequence and likelihood with assigned responsibilities. Identify and implement cost-effective controls where appropriate.
2	The CEO and Executive Committee to be informed on the status of this risk via scheduled reporting. General Manager to determine appropriate monitoring action and assign responsibility. GM to escalate by exception reporting to EC if oversight input on the management of the risk is required.	Active monitoring to seek greater clarity on the consequence and likelihood with assigned responsibilities. Identify potential for cost-effective controls where appropriate.
3	GM to Scheduled reporting to EC	Manage by appropriate internal controls and scheduled review when requested to confirm continued relevance and priority status.
4	Scheduled reporting to EC..	No active action or specific application of resources is required. Basic monitoring and review when requested to confirm continued relevance and priority status.

Table 2. Risk reporting, escalation, and monitoring

#### *Escalation*

Group Managers must escalate an emerging risk if the level of priority changes or other circumstances need to be brought to the attention of the Executive Committee as outlined in Table 2.

#### *Closure*

An emerging risk will be closed when any of the following occurs:

- No further action is required:
  - It no longer meets the emerging risk criteria.
  - The level of risk to Comcare is considered so low it no longer requires monitoring.
- Changed status for inclusion on a Strategic, Operational or Group Risk level:
  - The risk is no longer emerging as it may be captured in a strategic, operational or group risk register for oversight and reporting.
  - A project is established to manage the current risk and oversight will be provided by EPMO.

Closure of an emerging risks must be approved by the Executive Committee. Closed risks will be listed in a separate section of the register as shown at Table 5. An example of a completed entry is provided in Table 6.

The Finance and Assurance Team will update the Emerging Risk Register and coordinate any follow up action, ie ensuring the inclusion within the relevant strategic, operational or group risk register.



## Emerging Risk Template

Add a row for each new emerging risk.

ID	Date Added (Year/Month)	Emerging Risk	Lead Group responsible	Source	Description	Strategic Risk Focus Area	Strategic Priority	Priority			Action (Responsibility/Due date)
								Time Horizon	Impact	Rating	
#	Date when first entered on the register eg 2023/01	Provide a short title	Use abbreviation ie Claims, ROG, Legal, Corporate, Scheme or SPE	Select from the following: • Bills/Policy Initiatives • Legislative amendments • Parliamentary Inquiries • Reforms • Changes in Government or policy agenda • External Reviews • Social • Economic • Technological • Other (i.e licensee insolvency)	Provide a description of the emerging risk, including how it has arisen, the relevant stakeholders and how it affects Comcare. Potential threat or opportunity or considerations for both?	<input type="checkbox"/> Capability <input type="checkbox"/> Governance <input type="checkbox"/> Culture <input type="checkbox"/> Stakeholders	<input type="checkbox"/> Excellence in service provision <input type="checkbox"/> Engagement with our stakeholders <input type="checkbox"/> Prevention & early intervention across our scheme <input type="checkbox"/> Insight driven & risk & evidence based practice <input type="checkbox"/> Being adaptive & sustainable in the face of change	<input type="checkbox"/> Short-term (3-6 Months) <input type="checkbox"/> Mid-term (6-12Months) <input type="checkbox"/> Long-term (+12 Months)	<input type="checkbox"/> High <input type="checkbox"/> Moderate <input type="checkbox"/> Low	Refer to Priority Matrix. <input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4	List all actions Comcare will undertake to prepare for manage the emerging risk, including responsibility and due date.

Table 3. Emerging risk template

## EXAMPLE

ID	Date Added (Year/Month)	Emerging Risk	Lead Group responsible	Source	Description	Strategic Risk Focus Area	Strategic Priority	Priority			Action (Responsibility/Due date)
								Time Horizon	Impact	Rating	
1	2022/08	The Australian Public Service Commission (APSC) service-wide bargaining process	Corporate	Bills/Policy Initiatives	The APSC released the Public Sector Interim Workplace Arrangements 2022 in October 2022, which allows the Commission to consult on and develop the best approach to service-wide bargaining. Further the Public Sector Workplace Relations Policy 2023 has also been released. The process will to be conducted in two parts and will involve the appointment of Peter Riordan PSM CF to represent agencies as the APS- wide Chief Negotiator (Part A); and each department / agency will have their own Agency Lead Negotiator/s to lead bargaining on matters specific to agencies (ie non-common terms) (Part B). APSC has recently reached out to agencies to seek contact details for lead negotiators.	<input checked="" type="checkbox"/> Capability <input checked="" type="checkbox"/> Governance <input type="checkbox"/> Culture <input type="checkbox"/> Stakeholders	<input checked="" type="checkbox"/> Excellence in service provision <input type="checkbox"/> Engagement with our stakeholders <input type="checkbox"/> Prevention and early intervention across our scheme <input type="checkbox"/> Insight driven and risk and evidence based practice <input type="checkbox"/> Being adaptive and sustainable in the face of change	<input checked="" type="checkbox"/> Short-term (3-6 Months) <input type="checkbox"/> Mid-term (6-12Months) <input type="checkbox"/> Long-term (+12 Months)	<input type="checkbox"/> High <input type="checkbox"/> Moderate <input checked="" type="checkbox"/> Low	Refer to Priority Matrix. <input type="checkbox"/> 1 <input type="checkbox"/> 2 <input checked="" type="checkbox"/> 3 <input type="checkbox"/> 4	Comcare will respond to the Lead Negotiator request by the expected deadline. People Operations Team will support the lead negotiator and Comcare executive throughout the process of working with APSC and undertaking bargaining. Contact details to be provided by Nov 2022.

Table 4. Emerging risk template – example of an entry



## Closed Emerging Risk template

Add a row for each closed emerging risk.

ID	Date Added (Year/Month)	Emerging Risk	Lead Group responsible	Source	Description	Strategic Risk Focus Area	Strategic Priority	Outcome/Reason for closure	Closure date (Year/Month)
		Provide a short title	Use abbreviation ie Claims, ROG, Legal, Corporate, Scheme or SPE	Select from the following: • Bills/Policy Initiatives • Legislative amendments • Parliamentary Inquiries • Reforms • Changes in Government or policy agenda • External Reviews • Social • Economic • Technological • Other (i.e licensee insolvency)	Provide a description of the risk, including how it has arisen, the relevant stakeholders and how it affects Comcare	<input type="checkbox"/> Capability <input type="checkbox"/> Governance <input type="checkbox"/> Culture <input type="checkbox"/> Stakeholders	<input type="checkbox"/> Excellence in service provision <input type="checkbox"/> Engagement with our stakeholders <input type="checkbox"/> Prevention and early intervention across our scheme <input type="checkbox"/> Insight driven and risk and evidence based practice <input type="checkbox"/> Being adaptive and sustainable in the face of change	Outline the outcome and reason for closure.	Eg 2022/02

Table 5. Closed emerging risk template

## EXAMPLE

ID	Date Added (Year/Month)	Emerging Risk	Lead Group responsible	Source	Description	Strategic Risk Focus Area	Strategic Priority	Outcome/Reason for closure	Closure date (Year/Month)
1	2022/08	The Australian Public Service Commission (APSC) service-wide bargaining process	Corporate	Bills/Policy Initiatives	The APSC released the Public Sector Interim Workplace Arrangements 2022 in October 2022, which allows the Commission to consult on and develop the best approach to service-wide bargaining. Further the Public Sector Workplace Relations Policy 2023 has also been conducted in two parts and will involve the appointment of Peter Riordan PSM CF to represent agencies as the APS-wide Chief Negotiator (Part A); and each department / agency will have their own Agency Lead Negotiator/s to lead bargaining on matters specific to agencies (ie non-common terms) (Part B). APSC has recently reached out to agencies to seek contact details for lead negotiators.	<input checked="" type="checkbox"/> Capability <input checked="" type="checkbox"/> Governance <input type="checkbox"/> Culture <input type="checkbox"/> Stakeholders	<input checked="" type="checkbox"/> Excellence in service provision <input type="checkbox"/> Engagement with our stakeholders <input type="checkbox"/> Prevention and early intervention across our scheme <input type="checkbox"/> Insight driven and risk and evidence based practice <input type="checkbox"/> Being adaptive and sustainable in the face of change	This is no longer an emerging risk. Service Wide bargaining has commenced. People Operations Team are supporting the lead negotiator and Comcare executive throughout the process of working with APSC and undertaking bargaining. This is now to be included in the Strategic Risk register.	2023/04

Table 6. Closed emerging risk template – example of an entry

### Nominated Group Contacts

All groups are to have one nominated point of contact for coordination of emerging risk identification and reporting to the Finance and Assurance team.

The nominated Group Contacts are as follows:

Group and Contact title	Current staff member
<b>Office of the CEO</b>	
Executive Officer	s 47F
<b>Corporate Management Group</b>	
Senior Assistant Director Governance, Risk and Assurance (for strategic governance and Audit and Risk Committee feedback)	s 47F
Director Corporate Communications and Strategy (for Executive Strategic Planning and Group Planning alignment)	s 47F
<b>Strategic Partnerships and Engagement Group</b>	
Executive Officer, Strategic Partnerships and Engagement Group	s 47F
<b>Regulatory Operations Group</b>	
Assistant Director, Strategy and Governance	s 47F
<b>Scheme Management Group</b>	
Director Scheme Strategy	s 47F
<b>Claims Management Group</b>	
Director Claims Strategy and Governance	s 47F
<b>Legal Group</b>	
Director Legal Practice Management	s 47F

Table 7. Group contacts for the emerging risk process



Australian Government

Comcare

**OFFICIAL**

# FRAUD INVESTIGATIONS MANUAL

APRIL 2020

VERSION 1.7

**OFFICIAL**

**OFFICIAL**

47E(d)

## TABLE OF CONTENTS

Fraud Investigations Manual .....	1
TABLE OF CONTENTS .....	3
<b>1. OPERATING FRAMEWORK.....</b>	<b>5</b>
1.1 Introduction .....	5
1.2 Legislative and Policy Framework.....	5
1.2.1 Fraud Control Framework .....	5
1.3 Delegated Authority to Investigate on Behalf of Comcare .....	6
1.3.1 Australian Government Investigation Standards 2011 .....	6
1.3.2 Key Legislation and Policies .....	6
1.4 Definition of Fraud .....	6
1.5 Comcare's Response to Fraud.....	7
1.6 Investigation of Fraud .....	7
1.7 Interagency Relationships .....	9
1.8 Ethical Standards.....	9
1.9 Media .....	10
<b>2. IDENTIFICATION OF FRAUD AND CASE SELECTION .....</b>	<b>11</b>
2.1 Introduction .....	11
2.2 Receipt of Allegations of Fraud and Non-compliance .....	11
2.3 Identifying the Relevance of Information Received .....	11
2.4 Case Assessment – Risk and Prioritisation.....	12
2.4.1 Risk Assessment Framework .....	13
<b>3. INVESTIGATION MANAGEMENT .....</b>	<b>13</b>
3.1 Introduction .....	13
3.2 Roles and Responsibilities .....	14
3.3 Investigation Plan .....	14
3.3.1 Investigation Objectives .....	15
3.3.2 Evidence Matrix .....	15
3.4 Investigation Management Aids .....	16
3.4.1 Operational Orders .....	16
3.4.2 Monthly Reporting .....	16
3.4.3 Monthly Case Reviews .....	16
3.5 Recording Investigative Activities.....	16
3.5.1 File and Information Management .....	16
3.5.2 Critical Decisions .....	18
3.5.3 Investigator's Written Records .....	18
3.5.4 Electronic Recording .....	18
3.5.5 Case Conferences .....	19
3.5.6 Investigation Closure.....	19
3.5.7 Brief of Evidence (BOE) .....	19
3.5.8 Enforcement Committee.....	20
3.5.9 Finalising investigations .....	20

3.6 Quality Assurance Review ..... 21

4

7

E

(

d

)

... 37



## 1 OPERATING FRAMEWORK

### 1.1 Introduction

The Fraud Investigations Manual has been developed to provide relevant Comcare staff with clear information on their responsibilities and obligations when conducting fraud investigations.

The purpose of this manual is to ensure that Comcare delivers consistent practices in accordance with Commonwealth and Agency policies and standards for the management of fraud allegations and related investigations. Accordingly, this manual is aligned with the:

- [Public Governance, Performance and Accountability Act 2013 \(Cth\)](#)
- [Public Governance Performance and Accountability Rule 2014 \(Cth\)](#)
- [Criminal Code Act 1995 \(Cth\)](#)
- [Crimes Act 1914 \(Cth\)](#)
- [Commonwealth Fraud Control Framework 2017](#);
- [Commonwealth Resource Management Guide No. 201](#) “Preventing, detecting and dealing with fraud (the Fraud Guide);
- [Australian Government Investigations Standards 2011](#) (AGIS); and
- Comcare Policy Statement (Fraud Control Plan) and associated Agency requirements.

Assurance, Risk and Fraud within the Corporate Group is responsible for the investigation of allegations of fraud against Comcare. These allegations may relate to Comcare’s worker’s compensation scheme scheduled to the [Safety, Rehabilitation and Compensation Act 1988](#) (Cth) (**SRCA Act**), regulatory scheme scheduled to the [Work, Health and Safety Act 2011](#) (Cth) (**WHS Act**) or Comcare employees.

### 1.2 Legislative and Policy Framework

#### 1.2.1 Fraud Control Framework

The Commonwealth sets standards for preventing, detecting and responding to fraud in sections 15 to 19 of the *Public Governance, Performance and Accountability Act 2013* (Cth) (**PGPA Act**) and section 10 of the *Public Governance, Performance and Accountability Rule 2014* (Cth) (**PGPA Rule**). These sections outline fraud control requirements Comcare needs to adhere to for compliance with its obligations as a Commonwealth Corporate Entity under the PGPA Act.

The Commonwealth Fraud Control Framework outlines the Australian Government's requirements for fraud control, including that government entities put in place a comprehensive fraud control program that covers prevention, detection, investigation and reporting strategies. The framework consists of three key documents:

[Fraud Rule](#) – Section 10 PGPA Rules

[Fraud Policy](#) – Commonwealth Fraud Control Policy

[Fraud Guidance](#) – Commonwealth Resource Management Guide No.201 (CRMG 201) – preventing, detecting and dealing with fraud

Section 10 of the Fraud Rule articulates the key principles for establishing and maintaining fraud control systems, including prevention, detection and responses to fraud. CRMG 201 expands on these principles to articulate a flexible framework for fraud control that can be tailored to the circumstances and needs of different entities, while providing coherent, consistent, transparent and accountable requirements.

Whilst the Fraud Rule is mandatory for Commonwealth corporate entities, and the Policy and Guidance are listed as best practice, Comcare adheres to all requirements of the Commonwealth fraud control framework for effective fraud control with dedicated staff within Comcare working across the prevention, detection and investigation of potential fraud matters.

## 1.3 Delegated Authority to Investigate on Behalf of Comcare

Comcare's CEO (as the accountable authority of Comcare) has formally authorised appropriate Comcare staff to undertake fraud investigations or otherwise deal with incidents of fraud or suspected fraud for Comcare as required pursuant to section 10(e) of the PGPA Rules.

### 1.3.1 Australian Government Investigation Standards 2011

The Australian Government Investigation Standards (AGIS) are a cornerstone of the Australian Government's fraud control policy and set the minimum standard for agencies conducting investigations relating to the programs and legislation they administer. The AGIS apply to all stages of an investigation.

### 1.3.2 Key Legislation and Policies

Other key Commonwealth legislation and guiding documents that inform the management and investigation of fraud include:

- *SRC Act*
- *WHS Act*
- *Proceeds of Crime Act 2002 (Cth)*
- *Freedom of Information Act 1982 (Cth)*
- *Ombudsman Act 1976*
- *Privacy Act 1988 (Cth)*
- *Commonwealth Evidence Act 1995*
- *CDPP - Disclosure Policy*
- *CDPP - Search Warrant Manual (Volume 1 & Volume 2)*
- *CDPP - Guidelines on Brief Preparation*
- *CDPP – Prosecution Policy of the Commonwealth*
- *CDPP - Guidelines for Dealings Between Commonwealth Investigators and the CDPP*
- *CDPP – Guidelines for Commonwealth Agencies – Offers of Assistance to Authorities*
- *Guidelines for executing Search Warrants by the Australian Federal Police on behalf of Commonwealth Departments*
- *Public Service Act 1999 (Cth)*
- *Australian Public Service Values and Code of Conduct*
- *Comcare CEO Directions and Instructions*
- *Comcare Claims Policy and Procedures manual*

In addition, Fraud investigators are able to request legal advice from Regulatory Legal on interpretation, application or any aspect of relevant legislation and policy to assist in an investigation (all requests for legal advice must be approved by the Assistant Director Assurance, Risk and Fraud in the first instance).

## 1.4 Definition of Fraud

Comcare has adopted the following definition of fraud from CRMG 201:

"Dishonestly obtaining a benefit, or causing a loss, by deception or other means".

This definition includes:

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

A benefit is not restricted to monetary or material benefits, and may be tangible or intangible, including the unauthorised provision of access to, or disclosure of, information. A benefit may also be obtained by a third party rather than, or in addition to, the perpetrator of the fraud.

As outlined in CRMG 201, fraud against the Commonwealth takes many forms, and may target:

- revenue (e.g. income tax, premium payments, GST fraud, customs duties)
- benefits and transfer payment (e.g. income replacement payments (including obtaining through the provision of false information to medical specialist's – intentional malingering), medical expenses, aids and treatments, collusive behaviour between service providers and benefit recipients)
- property (e.g. cash, computers, other portable and attractive items, stationery)
- information and intelligence (e.g. personal information or classified material)
- Commonwealth programme funding and grants (e.g. education, childcare, employment)
- entitlements (e.g. expenses, leave, travel allowances, attendance records)
- government procurement through cartel conduct
- misuse of fraudulent identities (e.g. to access payments, services, information, locations or other benefits)
- facilities (e.g. unauthorised use of vehicles, information technology and telecommunication systems), and/or
- money or property held in trust or confiscated (e.g. bank guarantees, investments).

Common offence provisions that can be used in relation to fraud against Comcare functions are found in the following Acts:

- *Criminal Code Act 1995* (Cth)
- *Crimes Act 1914* (Cth)

## 1.5 Comcare's Response to Fraud

Comcare recognises that fraud is a critical business risk to the Agency and its functions. Fraudulent activity is unacceptable and must be dealt with in a timely, professional and coordinated manner. Comcare's Fraud Control Policy outlines its approach to fraud control. Comcare's associated policies and fraud control framework aligns with the Commonwealth Fraud Control Framework and the AGIS.

## 1.6 Investigation of Fraud

Under the AGIS, Commonwealth agencies are required to investigate less serious or complex offences against agency programs. This requirement includes investigations which may require an administrative remedy, or referral for consideration of criminal prosecution.

Given the changing scope and workload of the Australian Federal Police (AFP), the need for Agencies such as Comcare to investigate their own fraud matters also increases, as does the threshold at which matters can be referred to the AFP.

The Assurance, Risk and Fraud unit (**ARF**) is responsible for conducting robust assessment and investigation into allegations of fraud committed against Comcare and its schemes in accordance with the AGIS, ensuring all allegations are recorded, assessed and resolved appropriately.

The objective of ARF activities is to protect public money and property administered by Comcare and to protect the integrity, security and reputation of Comcare and its schemes. The objective of sanctions imposed as a result of investigations is to reduce losses and potential losses (savings) incurred through non-compliance with the law, recover money and property and deliver deterrence against fraud.

Where a matter meets the AFP's *Case Categorisation and Prioritisation Model* for acceptance to the AFP, the matter will be referred to the AFP. ARF will deal with all other matters.

ARF will provide regular updates to the Comcare Executive on the progression of fraud investigations. Data from investigative outcomes will be used to inform fraud prevention and control education activities.

ARF investigators do not have delegated powers under the SRC Act or WHS Act and rely on delegated officers of Claims Management Group, Regulatory Operations Group, Scheme Management Group and Corporate Group to provide information to progress investigations. Any further information collection must be conducted through Federal Agents of the AFP exercising powers scheduled to the *Crimes Act 1914* (Cth) or through the voluntary provision of information from relevant parties to an investigation.

## 1.7 Interagency Relationships

Comcare supports the whole of Government approach to combating fraud against Commonwealth agencies.

AGIS encourages agencies to foster interagency co-operation in Australian Government liaison forums and fraud investigations, especially where agencies are unable to adequately maintain investigation expertise or resources and require assistance.

Where an investigation identifies criminal activity involving another agency's activities or programs, ARF must report the matter to that agency subject to any requirements or limitations under the Privacy Act or other agency legislation (CRMG 201, section 10.33).

The requirements of the *Australian Privacy Act 1988* (Cth), in particular the Australian Privacy Principles (APPs), must also be considered when requesting or sharing information.

Generally, APP 6.2 (e) is utilised for the disclosure of personal information between agencies. This section allows the use or disclosure of personal information about an individual if the entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body. Whilst APP 6.2 allows the use or disclosure of the information, it does not compel an entity to provide information. Some agencies have specific legislative powers to obtain information. ARF employees have no such coercive legislative powers.

### Specific authorities to share information

- Australian Taxation Office (ATO) – Section 355-65 (Table 5) of the *Taxation Administration Act 1953* allows the Australian Taxation Office (ATO) to release ATO information to Comcare.
- Services Australia (Centrelink) – Similarly sections 208(1)(b)(i) of the *Social Security (Administration) Act 1999*, 168(1)(b)(i) of the *A New Tax System (Family Assistance)(Administration) Act 1999* and 355(1)(b) of the *Student Assistance Act 1973* allow Centrelink to disclose information to Comcare.

Agencies such as ATO and Centrelink have specific information gathering powers in their legislation to request information from Comcare. Written requests from these agencies must be complied with by law and be recorded on the case management system.

Allegations or intelligence received which does not relate to Comcare are to be forwarded to the appropriate agency.

The tabled State and Commonwealth Government agencies at Appendix A may provide further assistance in the investigation of fraud involving Comcare's schemes.

## 1.8 Ethical Standards

All Comcare employees including ARF are bound by the *APS Values* and *APS Code of Conduct*. A breach may result in a code of conduct investigation which could lead to formal misconduct action.

ARF employees are required to act in a legal and ethical manner during the conduct of investigations. They must comply with the legal and policy framework specified in section 1.2 of these procedures.

An investigation is the search for truth in accordance with the specifications of law and confines of policy in the interests of justice. Two legal principles operate in favour of persons suspected of an offence at law. They are:

- the presumption of innocence and

- the rule against self-incrimination.

47E(d)

\\



## **2 IDENTIFICATION OF FRAUD AND CASE SELECTION**

### **2.1 Introduction**

This chapter aligns with the AGIS and establishes the recommended minimum standards for agencies in receiving and evaluating referrals or conduct identified as allegedly, apparently or potentially breaching the law.

### **2.2 Receipt of Allegations of Fraud and Non-compliance**

Allegations of suspected fraudulent activities may be received from a number of sources, including:

- members of the public;
- Claims Compliance team;
- Comcare employees (including Claims Managers, Human Resources);
- other Commonwealth or State/Territory agencies (including RCMs);
- government or ministerial referrals;
- scheduled auditing processes;
- integrity or compliance processes; and
- intelligence activity.

There are a number of ways to report suspected fraud. The following options are available:

- Comcare external website 'Reporting Fraud' webpage
- A dedicated 1300 366 979 telephone number
- Comcare fraud inbox ([fraud@comcare.gov.au](mailto:fraud@comcare.gov.au))
- Public Interest Disclosures (*Public Interest Disclosure Act 2013* (PID Act))

A work flow has been prepared for the receipt and management of referrals.

47E(d)

47E(d)

s 47E

47E(d)

Comcare may also seek AFP assistance or advice in relation to an investigation being conducted into suspected breaches of Commonwealth legislation (i.e. Section 4.7 provides guidance for seeking AFP assistance in executing search warrants).

s 47E

### 3. INVESTIGATION MANAGEMENT

#### 3.1 Introduction

The chapter aligns with the requirements of AGIS, which establish the minimum standards for the effective and efficient management of investigations. These recommended minimum standards will ensure Comcare can withstand scrutiny of mandated investigative processes, which can occur through court or tribunal processes, the media, the public and Government.

AGIS defines an investigation as<sup>1</sup>:

*“An investigation is a process of seeking information relevant to an alleged, apparent or potential breach of the law, involving possible judicial proceedings. The primary purpose of an investigation is to gather admissible evidence for any subsequent action, whether under criminal, civil penalty, civil, disciplinary or administrative sanctions. Investigations can also result in prevention and/or disruption action.”*

The ‘case management’ of investigations requires a pragmatic approach, supported by electronic systems and manual processes. The adoption of appropriate planning tools and standards ensures cases are managed and investigated in an efficient and cost effective manner. Review and continuous improvement initiatives are also critical components.

Investigation case management is based on the general principles of project management. However, it should be noted that the major difference between project management and investigation management relates to projected outcomes. While project management aims for an acceptable and pre-determined, or fixed outcome, investigation management outcomes are inherently variable. Consequently, Comcare investigators must be flexible and responsive to risks and related opportunities, such as changes in the scope of an investigation through the opening of new and unexpected lines of inquiry.

47E(d)

Comcare Investigators must adhere to case management principles and disciplines and consistently utilise investigation case management tools in all investigations. Systematic application of these planning, decision making,

---

<sup>1</sup> Australian Government Investigation Standards (AGIS) 2011, p1.

review and reporting procedures will facilitate transparent and logical decision making as well as ensuring ongoing 'quality control' of investigations.

### 3.2 Roles and Responsibilities

The roles and responsibilities listed below are limited to relevant staff members within the Assurance, Risk and Fraud unit, who have responsibility to detect or investigate fraud.

**Chief Finance Officer (CFO)** – is responsible for oversight and leadership of the Finance and Assurance team, including the Assurance, Risk and Fraud Unit.

**Assistant Director – Assurance, Risk and Fraud** – is responsible for developing and implementing Comcare's Fraud Control Framework and overall management of the Assurance, Risk and Fraud unit, including the investigative function.

**Principal Investigator – Assurance, Risk and Fraud** – is responsible for undertaking investigations and the allocation, management and quality assurance of all investigation casework, providing guidance to Investigators and regularly reporting to Senior Management (through the COO).

- Minimum qualification for this position – Diploma of Government (Investigations).

**Senior Investigator – Assurance, Risk and Fraud** – is the case officer allocated the case and principally responsible for the progression and outcome of investigations.

- Minimum qualification for this position – Certificate IV in Government (Investigations).

**Investigations Support Officer – Assurance, Risk and Fraud** – is responsible for recording and evaluating fraud allegations and supporting the administration of the Assurance, Risk and Fraud team.

**Senior Fraud Control Officer – Assurance, Risk and Fraud** – is responsible for supporting the implementation of Comcare's Fraud Control Framework and coordinating the maintenance of fraud risk assessments, to inform the Comcare fraud control environment and investigative activities.

- Desirable qualification for this position – Certificate IV in Government (Fraud Control).

All members of the investigation team contribute to, and share responsibility for, the progression and outcome of cases. However, it is the responsibility of the Principal Investigator and Senior Investigator to ensure a case is completed in an efficient and effective manner.

47  
E(  
d)

### 3.3.1 Investigation Objectives

The primary objective of an investigation plan is likely to be ‘to establish if any offence has been committed’, or ‘to seek evidence to prove, or disprove...’ or similar. The secondary objective may be to ‘identify agency risks’. Setting the initial objective establishes the general direction of the investigation. Objectives must be clear, and continue to be revisited as the investigation progresses and revised if required. Specific details of the allegation under investigation must be built into the objective. Where the nature of the allegation changes, then the investigator should discuss with the Principal Investigator whether a Critical Decision Record should be completed, or, where the change is of such a significant degree that a new investigation plan may be required.

An example of an investigation’s primary objective could be: *‘To establish whether an offence against section 134.2 of the Criminal Code Act 1995 (obtaining a financial advantage by deception) has occurred’*. Setting the initial objective establishes the general direction of the investigation. It is quite possible for several offences (or Acts) to be considered in this document.

### 3.3.2 Evidence Matrix

The development of an Evidence Matrix flows naturally from the primary objective(s) of an investigation. While setting the initial objective provides general direction, preparing an Evidence Matrix develops a more detailed roadmap – identifying potential ‘lines of enquiry’ and acting as a blueprint for the evidence collection phase of an investigation.

An Evidence Matrix will identify the:

- suspected offending parties;
- possible breaches or offences;
- elements (proofs) of the breaches or offences;
- evidence required to prove those elements; and
- potential location/source of the required evidence.

Preparation of an Evidence Matrix is fundamental to both the planning and conduct of an effective investigation as this:

- reduces the risk that crucial evidence or lines of enquiry may be overlooked or tainted;



- directly informs action planning, resource requirements and the estimation of investigation complexity and costs; and
- provides an invaluable 'check-list' for the preparation and compilation of a Brief of Evidence.

In some simple and straight forward matters, an Evidence Matrix may not be required (with agreement of the Principal Investigator). In most matters, however, an Evidence Matrix must be prepared by the Case Officer and annexed to the Investigation Plan.

### **3.4 Investigation Management Aids**

During the course of an investigation there may be extensive operational activity requiring sound management practices and accountable decision-making. A number of operational aids are provided below, to facilitate the effective conduct of such activities. Templates have been developed for each of these aids.

47E(d)



Investigator in the first instance. For procedures relating to the management of general files, refer to Comcare's records management policy.

47E(d)

#### **3.5.4 Electronic Recording**

Legally, using a tape/audio recording device to make notes is acceptable as a note taking tool. The use of such devices must be in accordance with relevant State/Territory '*Listening Devices*' legislation. In most jurisdictions the covert recording of another person is either illegal or subject to stringent legal requirements.

To this end, the ARF will take a pro-active, model litigant approach.

ARF Investigators:

---

<sup>2</sup> Australian Government Investigation Standards (AGIS) 2011, p10.

- **will not** use 'note taking electronic audio recorders' covertly. Use will always be overt, that is the person whose conversation is being recorded has knowledge that the recording is taking place and has provided their consent. This consent will form part of the recording.
- Must ensure that they are personally confident and competent in the use of the equipment.
- If the equipment is used to tape conversations with witnesses and potential suspects, it should be remembered that cautioning and rights in accordance with part 1C of the *Crimes Act 1914* will apply once the investigator suspects the person may be complicit in the offences. Suspects will normally be interviewed using the formal Record of Interview (ROI) facilities.
- Must ensure that when electronic notes are created and/or relevant conversations are recorded, those records are appropriately maintained and stored.
- Where a digital device is used, ensure downloading of the record onto a 'read only' disk is completed as soon as possible.
- Ensure that one 'original' disk is then secured as per standard evidence handling and storage protocols. (A reference in the investigators official notebooks should be made of the recording and the fact that this method was adopted).
- There is no requirement to immediately fully transcribe those recordings, however, the CDPP may require that to occur at a later date – (Full disclosure).
- Ensure that the complete process is described in the investigators witness statement (and if applicable, also recorded in the corroborators statement).

47E(d)

47E(d)

### 3.5.7 Brief of Evidence (BOE)

All briefs must comply with the following;

- applicable laws of evidence
- rules of court applicable to the jurisdiction where litigation takes place
- *Prosecution Policy of the Commonwealth*
- *CDPP Guidelines on Brief Preparation*

- *CDPP e-Brief Template Instructions*
- *Legal Services Directions 2005*
- *Guidelines on Disclosure to CDPP by Investigative Agencies*
- Applicable disclosure requirements in the jurisdiction

47E(d)

47E(d)

47E(d)



47E(d)

### **3.6 Quality Assurance Review**

Comcare management must be assured that investigations are conducted in an efficient and effective manner, and meet contemporary standards and expectations such as those prescribed in the AGIS. Management must also be assured that critical decision-making during investigations is robust and transparent.

An effective means of measuring levels of compliance is to conduct Quality Assurance Reviews (QARs) in accordance with AGIS requirements. The COO will request a QAR be conducted by:

- The AFP where Comcare is unsuccessful in seeking prosecution following a referral to the CDPP.
- From another agency with suitable skills and capacity, where an investigation fails to get sufficient evidence to refer a matter for prosecution.

## **4. INVESTIGATION PRACTICES**

### **4.1 Introduction**

This chapter aligns with the AGIS requirement for robust investigation practices, and establishes the recommended minimum standards in regard to:

- Managing witnesses and persons of interest
- Conducting search warrants
- Obtaining, recording and storing relevant and admissible evidence.

### **4.2 Human Information Sources**

Human sources are people who supply or agree to supply information to the agency in relation to investigations and their identity may need to be protected due to the likelihood of that person being put at risk.

Comcare does not use human information sources of the kind referred to in the AGIS. However Comcare does receive information from anonymous informants, to which the provisions of the FOI Act, public interest immunity and the Privacy Act apply.

## 4.3 Witness Management

A witness is any person with knowledge of a matter who is capable and competent to give evidence at judicial proceedings. The rights and interests of witnesses must be respected at all times. ARF investigators must maintain appropriate communication with witnesses before and after interviews and, where suitable, keep witnesses informed of progress of investigations, especially in the lead up to court hearings where they might be required to provide evidence.

### 4.3.1 Preparing for Witness Interview

s 47E

Witness statements can be obtained electronically or in person. Witnesses should be contacted for a statement at the earliest opportunity to retain the contemporaneous nature of their information. The investigator is to determine the most appropriate means for taking the witness statement based upon the nature of the witness, the information they can provide, their location and their availability. s 47E

#### Expert witness

A witness is considered an expert under the *Evidence Act 1995* where they are able to demonstrate the requisite expertise obtained through their experience, training or study. ARF investigators will seek expert assistance when they do not have the necessary technical expertise in a given field. The selection of an expert will be made following consideration of the person's standing, qualifications, capabilities and relevant experience to establish the necessary credibility before the court or tribunal.

Where an expert witness is to provide evidence, the expert witness's statement will provide a full list of their formal qualifications and a summary of their relevant experience.

If an expert witness is required, the investigator is to prepare a case conference brief, updated evidence matrices, and request a meeting with Regulatory Legal, the Principal Investigator and the Assistant Director ARF to gain approval.

#### Child witness and witnesses with a poor understanding of English

There are special requirements for people aged less than 18 years of age to have a responsible adult present during the interview and to co-sign any statement. People of non-English speaking background and Aboriginal and Torres Strait Islanders (ATSI) should be offered the services of an interpreter. Investigators also need to be aware of the Anungra rules in relation to Aboriginal Torres Strait Islander (ATSI) persons.

#### Hostile witness

s 47E

If the witness gives contrary evidence in a court or tribunal, CI investigators can be called to provide evidence of a prior inconsistent statement.

## 4.3.2 Statements

The format of a witness statement must be consistent across all CI investigations and comply with the applicable requirements of the jurisdiction where any court proceedings will occur.

Technical terms, slang and jargon used by a witness will be recorded in the statement and clearly explained to ensure there is a common understanding of the meaning. Investigators should undertake to use the phraseology of the witness in the statement.

All witness statements should be paginated, and every paragraph should be numbered using alphanumeric numerals.

Witness statements should contain the following:

- **Date:** The statement/affidavit must be dated. The date under the signature on the last page is the date the statement is signed by the witness.
- **Heading:** “Statement in the matter of ...”
- **Personal Details of Witness:** The full name, address, occupation and contact numbers of the witness will be recorded. In circumstances where the witness has concerns with providing their address in the statement, it may be omitted using the phrase ‘Known to Investigator’ or ‘Resides in the state of xx’. In the case of a witness who is providing evidence as part of their official duties, it is sufficient to provide their professional address. The residential address and telephone numbers of the witness should **NOT** be provided to the defence.
- Different jurisdictions have different requirements around certain aspects of a witness statement. For example, in NSW the statement must contain a person's age rather than their date of birth.
- **Format:** If practicable a witness statement should be typed and each paragraph should be numbered. Where a hand-written statement has been provided by a witness, an unsigned-typed version should be included in any brief of evidence, with a copy of the signed original document attached, to assure understanding.
- **Jurat:** A witness statement must include a jurat which is required by the jurisdiction where court proceeding is likely to occur. Examples of statement format and jurat relevant to each of the jurisdictions within Australia are provided below:
  - [ACT](#)
  - [NSW](#)
  - [NT](#)
  - [QLD](#)
  - [SA](#)
  - [VIC/TAS](#)
  - [WA](#)
- **Preamble:** The preamble establishes the context for the main body of the witness evidence, incorporating where they were, what they were doing, times, dates, etc. This could also include explanations of duties or procedures undertaken in areas of employment, which may be relevant to the matter under investigation.
- **Body:** Includes all relevant observations and conversations relevant to the elements of the offence being investigated.
- **Conversations:** Relevant conversations should be recorded in the first person, i.e. “I said... He said ...” If a witness is unable to recall the exact conversation, the phrase “Words to the effect” or “I can’t recall the

exact words however...” may be utilised prior to setting out the witness recollection of the conversation in the first person.

- **Exhibits:** Where relevant, a witness statement must fully describe physical exhibits and ensure that all handling of these is fully described to ensure evidence continuity is presented.
- **Signature of Witness:** There is no legal obligation for a witness to sign a statement. If the witness declines to sign the statement, the ARF investigators will note the fact that the request was made, and any reasons offered for declining.

Local legislation may require that a Justice of the Peace, a Police Officer or other specified person witness the signature of the person making the statement. ARF investigators must be conversant with the provisions of any relevant Evidence Act or other laws relevant to the jurisdiction in which the matter may proceed at court, and must ensure that requirements applicable in the jurisdiction where the matter will be heard are satisfied.

#### **Supplementary Statements**

If a witness wants to change part of their statement or add further information after signing, a supplementary statement must be prepared. The original statement and any supplementary statements **must** be retained for 47E(d)

## **4.4 Managing ‘Persons of Interest’**

When dealing with persons suspected of committing an offence (i.e. ‘persons of interest’), ARF investigators will ensure they act ethically and afford procedural fairness.

### **4.4.1 Formally Interviewing Persons of Interest**

The primary purpose of a formal record of interview is to afford procedural fairness by providing a person of interest with the opportunity to respond to any allegations. <sup>s 47E</sup>

s 47E

ARF Investigators must have a detailed working knowledge of, and apply, the Fraud Investigation Manual's standards and procedures, interview techniques and relevant legislation, including:

- The interviewer must have the minimum qualifications as required by AGIS, Certificate IV in Government (Investigations).
- The interviewer must have the appropriate authorisation from the CEO to undertake fraud investigations for Comcare or Seacare as appropriate.
- Where exhibits are referred to during the ROI, each exhibit should be marked with and audibly identified by a unique identifier.
- If a transcript of the ROI is made, the investigator must check the transcript for accuracy against the recording. A copy is then provided to the suspected offender.

s 47E

s 47E

s 47E

#### **Preparing for a formal record of interview**

In most instances, prior to commencing a formal record of interview with a person of interest, ARF investigators should send a letter to the person formally notifying them that an allegation has been made concerning them, broadly describing the nature of that allegation, and providing them with an opportunity to respond to the allegation in a formal record of interview.

s 47E

#### **Lead Investigator**

s 47E



s 47E

## **Corroborator**

s 47E

## **Use of Interpreters**

Where an ARF investigator is aware that a person of interest is unable, because of inadequate knowledge of the English language or a physical disability, to communicate orally with reasonable fluency in that language, the investigator must, before starting to question the person, arrange for the presence of an interpreter and defer the questioning until the interpreter is present.

ARF investigators must ensure:

- The interpreter is independent of the matter under investigation.
- The interpreter is aware of their obligation to translate the exact words used by the ARF investigator and the person of interest. The interviewer must ensure that the English translation is in the first person.
- Where possible, all formal interviews involving the use of an interpreter should be digitally recorded so they may be independently interpreted, if required.
- The interviewer should satisfy themselves that the interpreter appears to have no problem in conversing with the person of interest.

## **4.5 Search Warrants**

### **4.5.1 Introduction**

The purpose of this section is to provide guidance in the process involved in applying for, planning and seeking assistance from the Australian Federal Police (AFP) or a State/Territory Police agency in the execution of search warrants.

A search warrant is a document issued under authority of law, which authorises the holder to enter and search premises or sometimes to search a person, and (normally) to seize evidential material. It is an investigative tool used

where there are reasonable grounds to suspect that the proposed search will produce evidential material in relation to an offence under investigation.

### **Section 3E Search Warrants**

For the purposes of fraud investigations in the Commonwealth, the main search warrant provision is provided for under Section 3E of the *Crimes Act 1914*. Section 3E applies to all offences against Commonwealth law and State offences with a Commonwealth aspect.

Section 3E search warrants can be obtained to search premises and people. The legal definition of 'premises' includes a place or a conveyance (vehicle). A search warrant authorises entry onto the identified premises without the consent of the lawful occupier.

An ARF Investigator can make application for a section 3E search warrant; however, a search warrant can only be issued to an AFP Federal Agent or a State/Territory Police Officer (the 'Executing Officer'). The Executing Officer is legally responsible for executing the warrant and, for this reason, acts as the Team Leader controlling the overall warrant.

The application for a search warrant is made by way of an affidavit to an 'issuing officer'. An issuing officer is defined as being:

- a Magistrate
- a Justice of the Peace or other person employed in a court of a State or Territory who is authorised to issue search warrants.

An application is normally made in the State or Territory where the search warrant is to be executed unless there are circumstances that prevent this occurring.

#### **4.5.2 Preparing and Applying for Search Warrants**

A decision to apply for a section 3E search warrant is considered a critical decision and requires approval by the Principal Investigator, at a minimum. For sensitive cases, this decision might be escalated to a General Manager. A Critical Decision Record must be completed according to this manual.

### **Applying for police assistance**

The ARF Investigator is to prepare a formal request for search warrant assistance, for submission to the AFP or State/Territory Police agency. When seeking the assistance of the AFP or a State/Territory Police agency in the execution of a section 3E search warrant, the ARF Investigator must provide the agency with:

- the purpose of the search warrant;
- the reason why a search warrant is needed;
- the circumstances of the alleged offence(s);
- the proposed timing of the search warrant; and
- relevant contact details.

Requests for search warrant assistance from the AFP must be submitted to the AOCC using an AFP Referral Form.

NOTE - The AFP require requests to be provided to the relevant AOCC at least 14 days before the warrant is intended to be executed, although where circumstances permit the AFP will give urgent requests priority. In addition, the AFP requires the request for assistance to specifically state that the seizure of the evidential material is wholly for the purpose of a criminal prosecution and/or related action under the *Proceeds of Crime Act 2002* and not a disciplinary, administrative or civil proceeding.

On receipt of a written request the AFP will assess the request and advise Comcare if it has been accepted, if further information is required, or that the AFP is unable to assist. Where possible, the AFP will give priority consideration

to urgent requests. When a request is accepted, the AFP will provide the agency with the name and contact details of the intended AFP executing officer.

In assessing whether the AFP will accept a request from an agency for assistance in the execution of a search warrant, the following factors may be taken into account as part of the evaluation/assessment process:

- AFP capacity/resources to provide the assistance at the time and place required.
  - Comcare's clear intention to undertake a criminal prosecution.
  - Comcare's capacity to comply with the AGIS, particularly in relation to investigator qualifications, exhibit control, storage, security and disposal procedures.
  - Comcare's agreement to provide appropriate resources whether human, material or financial.
  - s 47E
- .
- In all the circumstances, whether the execution of a search warrant is the most appropriate course of action to pursue at the time.

Any AFP requests for further information or other relevant instructions must be met before the request can be considered.

### **Applying for Search Warrants**

The ARF Investigator<sup>3</sup> should prepare and apply for a search warrant in accordance with the Director of Public Prosecutions (DPP) *Search Warrants Manual* relevant to the State/Territory jurisdiction in which the Case Officer will be seeking the search warrant.

The ARF Investigator should consult with the Executing Officer (and the CDPP if required) prior to obtaining a search warrant. The Executing Officer may ask the ARF Investigator to make further inquiries if there are concerns about the adequacy of information contained within the search warrant. Further advice may need to be sought from the CDPP in relation to issues such as multiple warrants, the search of vehicles and individuals, and proceeds of crime/asset forfeiture provisions.

The search warrant should be obtained and all relevant planning aspects of the warrant execution settled 48 hours before the anticipated time of execution. In consultation with the ARF Investigator and/or the CDPP, the Executing Officer will determine the most appropriate arrangements to make the formal warrant application.

**NOTE:** The ARF Investigator, who is responsible for preparing and swearing the affidavit for the search warrant, must be present at the execution of the warrant.

### **4.5.3 Planning and Executing Search Warrants**

The planning and execution of a search warrant is the primary responsibility of the Executing Officer. The Executing Officer will at all times be responsible for the search warrant execution, seizure of evidential material/items and control of the warrant and premises.

---

<sup>3</sup> ARF Investigators applying for a section 3E search warrant must hold a Certificate IV in Government (Investigations).

The ARF Investigator should work closely with the Executing Officer in preparing Operational Orders, which assist in the coordination of all personnel and resources to be used in the application for, and execution of, a search warrant (for more information on Operational Orders, refer to section 3.6.1).

Key considerations in planning for a search warrant application and execution include:

- Making advance contact with the local Magistrate to book an appointment for warrant application (locally based AFP Federal Agents can sometimes assist with this).
- Pre-briefing with the Executing Officer, including roles and responsibilities outlined as per the Operational Orders.
- Logistics such as staff requirements and travel arrangements, including accommodation and vehicles, search warrant kits, stakeholder liaison/negotiations, safety and special needs.
- Execution of warrant (timings, roles & responsibilities). **NOTE:** the execution strategies will be largely determined by the Executing Officer.

s 47E

The Executing Officer will discuss with the ARF Investigator<sup>s 47E</sup> whether the Property Officer will be a ARF Investigator or a Federal Agent/Police Officer.

## Internal Notification of a Search Warrant

When a search warrant is being executed as part of a Comcare investigation, it is essential that appropriate and timely advice is provided to Senior Management and other necessary stakeholders. This may involve the provision of information prior to, during and following the execution of a search warrant. The ARF Search Warrant Notification procedure should be followed at all times, determining who, when and how stakeholders are to be notified. The completed notification plan is to be approved by the COO and attached to the Operational Orders.

s 47E

## Evidence Management

To preserve the evidentiary value and integrity of items seized as evidence in the course of executing a search warrant, ARF Investigators must strictly comply with the procedures prescribed in Section 4.8.6.

s 47E

#### Post Search Debrief

The requirement for a post execution debrief will be determined by the Executing Officer and ARF Investigator.

## 4.6 Evidence and Exhibits

### 4.6.1 Introduction

This section prescribes duties, responsibilities and procedures in relation to the custodial requirements for all physical evidence and exhibits. They are designed to ensure ARF:

- can account for evidence/exhibits and other relevant documents in its possession;
- has in place a system to help preserve the integrity of evidence/exhibits and other relevant documents;
- can store information about evidence/exhibits and other relevant documents so as to assist in the process of investigation; and
- meet its legislative responsibilities regarding the use and storage of sensitive information.

Whilst the terms 'evidence' and 'exhibits' can be interchangeable, for the purpose of this section the terms are applied as follows:

- **Evidence** - any item/document collected, or seized under warrant, during an investigation. Whilst the item/document is held by a Property Officer it will be referred to as evidence until its lodgement into the exhibit system by an Exhibit Registrar.
- **Exhibit** - any evidence that is lodged with the Exhibit Registrar. Once signed into the Exhibit Register, the evidence is referred to as an 'exhibit'.
- **Miscellaneous Property** – any item/document obtained through the course of an investigation that has not yet been identified as a specific exhibit but has been lodged into the Miscellaneous Property system to assure security and continuity.

All physical evidence and exhibits should be subject to the same procedures for handling, storage and destruction, as prescribed in this section, regardless of the manner in which they were obtained.

The outcome of a prosecution is dependent upon the strength of the evidence presented to the Court to substantiate charges. The rules of evidence prescribed in the Commonwealth *Evidence Act 1995* and equivalent State and Territory Evidence Acts will determine admissibility of evidence in judicial proceedings.

All CI staff who handle evidence must strictly follow the procedures prescribed in this section to ensure evidence can be admitted in judicial proceedings. These procedures are consistent with the Commonwealth guidelines and standards listed below:

- *AFP National Guidelines on Property and Exhibits*
- *HOCOLEA Best Practice Guidelines for Document Handling*
- *Australian Protective Security Manual*
- *Guidelines for the Execution of Search Warrants by Australian Federal Police on behalf of Australian Government Departments and Agencies*
- *Australian Government Investigation Standards (AGIS)*



- *Commonwealth DPP Search Warrant Manual*
- *General Guidelines between the Australian Federal Police and the Law Council of Australia as to the Execution of Search Warrants on Lawyer' Premises, Law Societies and like Institutions in Circumstances where a Claim of Legal Professional Privilege is made.*

#### **4.6.2 Evidence Management**

s 47E

Once an item has been taken into custody as evidence, it is essential that investigators are able to demonstrate the continuity of this evidence, thus maintaining the integrity of its evidentiary value. It is therefore mandatory that all procedures prescribed in this section are strictly adhered to when handling evidence and exhibits.

ARF Investigators should be familiar with the following in relation to evidence handling:

- Part IAA, Division 4C of the *Crimes Act 1914*: using, sharing and returning things seized.
- Part IAA, Division 2 of the *Crimes Act 1914*: the handling of things seized.
- The ongoing responsibilities of Executing Officers regarding the custody of material seized pursuant to search warrant, right through to its appropriate disposal.

#### **4.6.3 Use and Disclosure of Things Seized Under Search Warrant for Administrative Purposes (Part 1AA Crimes Act 1914)**

It is critical that information which is seized under a 3E Crimes Act warrant is only used for the purpose of that warrant, and not another purpose. Material seized under warrant must not be used for administrative decisions or functions, except under the following outlined circumstances.

##### **Use and disclosure of things seized under warrant**

A search warrant permits the seizure of things which are relevant to an offence. Things seized under a warrant are generally made available to Comcare investigators by police for the purposes set out in s 3ZQU of the *Crimes Act 1914*. It is important that ARF investigators taking possession of seized things read and understand the relevant provisions within Part IAA of the *Crimes Act 1914*. Section 3ZQU is particularly relevant in this context. It permits the use and disclosure of seized things where necessary for a number of specified purposes, one of which is the prevention, investigation and prosecution of Commonwealth offences.

##### **Using seized things to prevent, investigate and prosecute criminal offences**

Things seized under a warrant may be used by Comcare if it is necessary for the purpose of preventing, investigating or prosecuting an offence under Commonwealth law: *Crimes Act 1914*, s 3ZQU(1)(a). s 47E

#### **Investigation and prosecution**

The use of seized things by Comcare may include, where it is necessary and appropriate, showing some seized things to other persons, for the purpose of obtaining information or evidence to further the criminal investigation or to support a prosecution. s 47E

In that event, consideration should be given to the privacy and other interests of the person from whom the things were seized. Seized things should only be shown to others where necessary for the investigative/prosecution purpose. s 47E

If a copy of the seized thing is left with a witness, for example for analysis, arrangements should ordinarily be made for the copy to be returned when the person no longer requires access to it for the purposes of the investigation or prosecution. Witnesses should be reminded that it is not permissible for them to copy, use or disclose the information for purposes other than the investigation or prosecution.

#### **Preventing offences**

Similar principles apply in relation to the prevention of offences. s 47E

It is important that the safeguards discussed above in relation to the limited use of the seized material are also applied in relation to activities undertaken for the purpose of preventing offences.

**47E(d)**

47E(d)

#### **4.6.5 Evidence Management Records**

The continuity of evidence is maintained by taking accurate and consistent records of all evidentiary items, from collection or seizure, to examination by investigators and/or forensic specialists, to production as exhibits in court. The following describes the types of evidence records maintained by ARF when conducting evidence collection activities.

**NOTE:** when evidence is being seized in the execution of a search warrant, the Executing Officer will use Police equivalent evidence management records until the property is officially handed over to Comcare.

##### **Evidence Label**

An Evidence Label must be completed in relation to all collected evidence, and must be attached to the corresponding evidence bag or container. Each label requires the Searching Officer to record specific details in relation to the collected item, such as where it was located, a description of the item, the time and date collected, and the Searching Officer's signature. It also requires a unique identifying number which is based on the Searching Officer's initials, the owner/representative initials and sequential number of the item collected, e.g. JS - PB – 001.

**NOTE:** for evidence seized in the execution of a search warrant, the equivalent AFP or State Police barcode or other identifier is to be used and should not be changed.

##### **Evidence Receipt**

The Evidence receipt is a single form on which all details of the property seizure is recorded. This form must be completed by the Property Officer, detailing every item collected, using the identifying information recorded on each item's corresponding Evidence Label.

The Property Officer must invite the owner/representative to countersign the record as a receipt for the collected items. Either at the scene or immediately thereafter, a copy of the seizure record is to be provided to the owner/representative. (Smart phone scanning apps can facilitate the on-site capture and emailing of such documents in a .pdf format) The original copy of the Evidence Receipt is retained in the brief of evidence, with copies being used for exhibit lodgement or other investigation needs.

When evidence is lodged in the Compliance Investigations exhibit room, the lodging officer must make the Evidence Receipt available to enable a transfer of custody of the evidence to the Exhibit Room, in accordance with the procedures prescribed in Section 4.6.8.

### **Transfer of Evidence/Exhibit Record**

The Transfer of Evidence/Exhibit Record is also a single form, requiring signatures from both the officer handing over the property, and the person receiving it. A Transfer of Evidence/Exhibit Record must be completed by the responsible ARF Investigator for every transfer of evidence or exhibits. The record lists:

- the evidence/exhibit number and description
- the date of transfer
- the name of persons handing over and accepting the evidence/exhibit
- the reason for the transfer of custody.

The original Transfer of Evidence/Exhibit Record must be retained on the Case File (and may be required to be used in the Brief of Evidence). A scanned or otherwise copied version is given to the other party in the exchange.

A signed receipt must always be obtained from the person who takes possession of the item. Whenever an Executing Officer completes a Police equivalent Transfer of Evidence/Exhibit Record, a copy of this record/receipt must be obtained by the ARF Investigator accepting possession of evidence. The record/receipt is then retained to assist with recording the items in the Exhibit Register.

### **4.6.6 Collecting and Seizing Evidence**

When collecting evidence in the course of investigation field operations, or seizing evidence in the execution of a search warrant, the following steps must be followed to ensure the integrity and continuity of the evidence is maintained:

s 47E

#### **4.6.7      Legal Professional Privilege**

It is possible that some documents or digital evidence will be subject to legal professional privilege (LPP). It is important that the occupier of any such premises, or the person being searched, be given the opportunity to consider whether they should claim privilege on the document. Items subject to LPP should be dealt with in accordance with the *'General Guidelines between the Australian Federal Police and the Law Council of Australia as to the execution of search warrants on lawyers' premises, Law Societies and like institutions in circumstances where a claim of Legal Professional Privilege is made'*.

#### **4.6.8      Exhibit Management**

Exhibits form an integral part of an investigator's brief of evidence. Each exhibit must be accompanied by records which are able to demonstrate continuity of possession: from the time an item was collected or seized as evidence, its examination by a CI Investigator or technical expert, its production in a court as an exhibit, to its ultimate disposal.

It may not be necessary to retain all property regarded as exhibits, or to produce all exhibits to a court. Where possible, exhibits not forming the basis of a possible prosecution should be returned to the rightful owner or disposed of as soon as practicable. The decision to retain or dispose of an exhibit shall rest with the Case Officer (ARF Investigator).



## Exhibit Registrar<sup>4</sup>

The Agency Security Advisor has been appointed as the Exhibit Registrar and is responsible for the management of the Exhibit Room, and controlling the initial lodgement, and recording subsequent movement, destruction or return of evidence. The Exhibit Registrar is also responsible for physical access to the Exhibit Room in the normal sense.

Where an exhibit is stored in a designated exhibit room, it will be held in a security classified lockable cabinet.

On initial lodgement of exhibits, the Exhibit Registrar must:

- check that the item is contained in a correctly sealed evidence bag or container and is clearly labelled;
- where use of an evidence bag or container is not considered practical or possible, ensure that the item is sealed appropriately with an evidence seal or evidence sealing tape;
- verify the accuracy of each actual item with its description on the Evidence Receipt (or Transfer of Evidence/Exhibit Record or police equivalent); and

## Exhibit Register

The **Exhibit Register** is an A3 book with consecutively numbered pages. The Exhibit Register remains secured at all times in the Exhibit Room.

Subsequent movement of exhibits to and from the Exhibit Room are to be recorded against the relevant entry in the Exhibit Register.

## Handling and movement of exhibits

Exhibits may be required to be temporarily removed from the Exhibit Room for: examination by the Case Officer; examination by a third party (e.g. technical expert or forensic examiner); or for production in a court or tribunal. If an exhibit needs to be temporarily removed from the exhibit room, the following procedures apply under these circumstances:

*Case officer examination* - The removal and return of the exhibit must be recorded in the exhibit movement section of the Exhibit Register.

*Third party examination or production in a court:*

- The removal and return of the exhibit must be recorded in the exhibit movement section of the Exhibit Register.
- A Transfer of Evidence/Exhibit Record form must be completed for each movement and retained on the Case File.
- Exhibits should be 'safe hand' delivered to recipients, by an ARF Investigator, using a secure briefcase.

When a temporarily transferred exhibit is returned to the Exhibit Room, the Exhibits Registrar must:

- ensure the exhibit is contained in a correctly sealed evidence bag/container and is clearly labelled;
- ensure the item has been re-sealed by securing a new tamper evident seal (or tape) on top of the original seal; and
- complete the exhibit movement section of the Exhibit Register.

---

<sup>4</sup> Given the size of the CI team, there will be no specific Exhibit Registrar identified. All Investigators are to ensure they have an independent person with them when dealing with exhibits. Also, given there will be no specific Exhibit Registrar, there will be no need to keep a separate 'Exhibit Management File' for each matter. CI Investigators will ensure that a copy of each relevant exhibit documents is kept on the electronic file for ease of identification.

#### **4.6.9 Return or Destruction of Exhibits**

##### **Return to the Agency - Files**

Where documentary evidence obtained in the course of an investigation was provided by Comcare, the original document should, where possible, be returned to the files of origin, or if the file itself was the exhibit, returned to the relevant section following the conclusion of the investigation/prosecution. All Australian Government documents must be maintained in accordance with the *Archives Act 1983*.

##### **Return to Owner**

Subject to any contrary order of a court, an exhibit should be returned to its lawful owner if the reason for its collection/seizure no longer exists or the exhibit is not going to be used in evidence. This section does not apply to those things forfeitable to the Commonwealth or subject to a dispute of ownership.

The ARF Investigator (Case Officer) is responsible for ensuring the return of collected and seized exhibits and must contact the owner/representative in writing, requesting authorisation for return or destruction of the exhibits.

If the owner/representative authorises the return of the exhibits, the Case Officer must prepare a Transfer of Evidence/Exhibit Record which is to be signed by the recipient, with the original retained on the case file and a copy provided to the recipient.

The signed Authorisation for Return or Destruction of Collected/Seized Property is also to be retained on the case file.

##### **Destruction of Exhibits**

Exhibits can be destroyed, on completion of an investigation or legal proceedings, if:

- the owner of the exhibit has appropriately authorised the destruction of the exhibit, or
- an exhibit has no owner, or
- it would be unlawful to return the exhibit, or
- the exhibit is subject to a destruction order by a court

For destruction to occur, the ARF Investigator (Case Officer) must complete and have approved a Request for Approval to Dispose of Seized Property form and forward it to the Principal Investigator.

The Case Officer is responsible for:

- notifying the Principal Investigator of the authorisation of the destruction;
- recommending the method of destruction;
- providing the Principal Investigator with a 'Request for Destruction of Exhibit' form for approval; and
- retaining the original Request for Destruction of Exhibit form (and relevant attachments) on the Case File.

On receiving a Request for Destruction of Exhibit form, the Principal Investigator will:

- if agreed, authorise disposal of the exhibit and return to the ARF Investigator for actioning;
- Request that the destruction is witnessed by an independent person;
- Request that the ARF Investigator detail the date and location of destruction along with witness details;
- Request the ARF Investigator retain a copy of the completed Request for Destruction of Exhibit form on the case file.
- Request that the ARF Investigator update the Exhibit Register accordingly.

##### **Exhibit Room audit**

The Principal Investigator, or the Assistant Director ARF, will arrange for an audit to be conducted annually by an independent third party on the Exhibit Room.

Objectives of a complete or random audit include:

- an examination of the Exhibit Register for completeness and accuracy of entries;
- a physical sighting of exhibits;
- an examination of the wrappings and seals to ensure exhibit integrity;
- an opinion as to how well the exhibits are being managed; and
- recommendations regarding procedural amendments (if required).

The independent person conducting an audit must be accompanied and assisted by an ARF Investigator or the Exhibits Registrar at all times whilst in the Exhibit Room.

The independent person has the right to ask for records relating to any exhibit and may demand from any agency officer the production of an exhibit, document, record, register or other thing that is relevant to the audit process.

The Principal Investigator or Assistant Director ARF, will be notified in writing of the results of the audit by the independent person, and, as appropriate, implement any corrective measures necessary to ensure the integrity of the exhibit management process.

All working papers pertaining to the audit must be retained on file for future examination.

### **Integrity of Evidence Bags, Containers and/or Seals**

Tamper evident seals/tape are used to secure evidence bags and/or containers so the accountability and integrity of the evidence is preserved - sealing procedures help reduce any allegations of impropriety.

Seals should not be broken or tampered with prior to lodgement in the Exhibit Room. Once lodged in the Exhibit Room, the Case Officer must be on hand to supervise the breaking of seals for the following purposes:

- enable exhibits to be examined, separated, copied and/or catalogued;
- enable the owner of the seized items to observe the initial examination; or
- transfer custody of exhibits for forensic examination.

Any ARF Investigator opening an evidence bag for any reason should record in their Investigation Notebook the circumstances of the bag being opened. The record should include:

- the time/date and place that the evidence bag was opened;
- the name of the person opening the evidence bag;
- the name of the independent witness present while the evidence bag or container was being opened (if applicable);
- why the evidence bag was being opened;
- any inconsistencies in the evidence bag contents; and
- what occurred with regards to the handling of the contents of the evidence bag.

The ARF Investigator must ensure the original seal remains on the evidence bag or container, that the exhibit is returned to the same evidence bag or container, and a new tamper evident seal is applied and according to the procedures described above.

### **Safe Hand Delivery and use of Couriers**

'Safe hand' delivery of exhibits by ARF Investigators is the preferred method of delivery. ARF Investigators should use a Security Construction and Equipment Committee (SCEC) endorsed security brief case to carry the exhibits.

In special circumstances, exhibits may need to be transported to, or received from, remote locations. In these circumstances, a SCEC approved and secure courier service is to be used. When sending an exhibit through an approved courier service the transferring officer shall ensure that the exhibit is protected and packaged to

## OFFICIAL

preserve its evidentiary value. In all cases, the approval of the Principal Investigator should be sought before using a secure courier service to transport an exhibit.

When an item is returned to the owner or transferred to a third party, via an approved courier service, the ARF Investigator must include the following:

- exhibit(s) that are being returned/transferred;
- photocopy of the completed Transfer of Evidence / Exhibit Record;
- self-addressed return envelope (this will allow the signed Transfer of Evidence / Exhibit Record to be returned to the ARF Investigator); and
- a request for the return of the signed Transfer of Evidence / Exhibit Record via the enclosed envelope.

The ARF Investigator must retain the signed Transfer of Evidence/Exhibit Record and the courier's 'confirmation of delivery' on the Case File.

Name of Agency	Appendix A Role
<b>Commonwealth</b>	
<a href="#"><u>Australian Federal Police (AFP)</u></a>	The AFP enforces Commonwealth criminal law, and protects Commonwealth and national interests from crime in Australia and overseas. The AFP is Australia's international law enforcement and policing representative, and the chief source of advice to the Australian Government on policing issues.
<a href="#"><u>Attorney-General's Department (AGD)</u></a>	The AGD provides essential expert support to the Australian Government in the maintenance and improvement of Australia's system of law and justice.
<a href="#"><u>Australian Criminal Intelligence Commission (ACIC)</u></a>	The Australian Criminal Intelligence Commission (ACIC) is established under the Australian Crime Commission Amendment (National Policing Information) Act 2016 (Cwlth) as a statutory authority to combat serious and organised crime. Merging the ACC and Crimtrac, the ACIC is a niche, complementary agency that delivers specialist capabilities and intelligence to other agencies in the law enforcement community and broader government.
<a href="#"><u>Australian Cyber Security Centre (ACSC)</u></a>	The ACSC integrates the national security cyber capabilities across the Australian Signals, the Digital Transformation Agency, the Defence Intelligence Organisation, the Computer Emergency Response Team, the Cyber Security Policy Division of the Department of Home Affairs, ASIO, AFP, and the Australian Criminal Intelligence Commission cybercrime threat intelligence specialists. The Centre is also a hub for collaboration and information sharing with the private sector and critical infrastructure providers, state and territory governments, academia and international partners in order to combat cybercrime.
<a href="#"><u>Australian Government Solicitors</u></a>	The AGS are the leading lawyers to government in Australia. Broadly, the AGS has been providing legal services to government since Federation.
<a href="#"><u>Australian Health Practitioner Regulation Agency (AHPRA)</u></a>	AHPRA is the national regulatory of health practitioners. In the conduct of a fraud investigation, AHPRA may be able to share information in relation to a practitioner or may accept a referral from Comcare in relation to alleged non-compliance of a medical practitioner.
<a href="#"><u>Australian Postal Corporation (APC)</u></a>	APC is a government business enterprise providing postal services in Australia. APC can provide information in relation to PO Box ownership and entities receiving mail at a specified address.
<a href="#"><u>Australian Securities and Investments Commission (ASIC)</u></a>	ASIC is the national regulator of corporate, markets and financial services. ASIC can provide information in relation to all business and sole traders ever registered in Australia, including ABN's, ACN's, company structures, shares and insolvencies.
<a href="#"><u>Australian Trade and Investment Commission (Austrade)</u></a>	Austrade contributes to Australia's economic prosperity by helping Australian businesses. Austrade can provide information in relation to grants for Australian business and offshore trading of businesses.
<a href="#"><u>Commonwealth Director of Public Prosecutions (CDPP)</u></a>	The primary role of the CDPP is to prosecute offences against Commonwealth law, and to recover the proceeds of crime against the Commonwealth. The CDPP is responsible for the prosecution of alleged Commonwealth offences of fraud against Comcare programs and systems.
<a href="#"><u>Commonwealth Ombudsman</u></a>	The Commonwealth Ombudsman's services are available to anyone who has a complaint about an Australian Government agency which they have been unable to resolve.



<a href="#"><u>Department of Home Affairs</u></a>	The Department of Home Affairs has responsibility, in part, for national security, law enforcement, border control and immigration and can provide Comcare with travel movements and the immigration status of persons of interest.
<a href="#"><u>Department of Veterans' Affairs (DVA)</u></a>	DVA is a primary service delivery agency responsible for developing and implementing programs that assist the veteran and defence force communities. Similar to Comcare, DVA supports veterans through payments of pensions and medical expenses. As former defence employees are often eligible for SRC Act entitlements, DVA should be consulted if there is suspected overlap of claimed injuries.
<a href="#"><u>Fair Work Commission (FWC)</u></a>	FWC is Australia's national workplace relations tribunal and may need to be consulted for industrial relations information as it pertains to internal investigations.
<a href="#"><u>The Office of the Australian Information Commissioner</u></a>	The OAIC is an independent statutory agency within the Attorney General's portfolio and has three sets of functions around freedom of information, privacy and government information policy.
<a href="#"><u>Safe Work Australia</u></a>	Safe Work Australia's was established to lead policy development that improves work health and safety and workers' compensation arrangements across Australia. As a national policy body Safe Work Australia does not regulate work health and safety laws, however, can provide information in relation to WHS legislation.
<b>Queensland</b>	
<a href="#"><u>Queensland Police Service (QPOL)</u></a>	The QPOL serves the people of Queensland by preventing crime and upholding the law in a manner which has regard for the public good and the rights of the individual. The QPOL is the lead agency in the investigation of Queensland State offences of fraud against Comcare programs and systems.
<a href="#"><u>The Office of the Director of Public Prosecutions (ODPP)</u></a>	The Queensland DPP, on behalf of the community, prosecutes people charged with serious criminal offences in Queensland. The DPP is responsible for the prosecution of alleged Queensland State offences of fraud against Comcare programs and systems.
<a href="#"><u>WorkCover Queensland</u></a>	WorkCover Queensland (WorkCover) is an independent government owned statutory body responsible for managing state-based accident insurance claims for all employer's without Comcare cover or a self-insurance licence.
<b>New South Wales</b>	
<a href="#"><u>NSW Police (NSWP)</u></a>	The NSWP protects the community and property of NSW by preventing, detecting and investigating crime, maintaining social order and performing and coordinating emergency and rescue operations. The NSWP is the lead agency in the investigation of NSW State offences of fraud against Comcare programs and systems.
<a href="#"><u>NSW Office of the Director of Public Prosecutions (DPP)</u></a>	The role of the NSW DPP is to independently advise in, review, institute and conduct prosecutions in criminal matters and to maintain and improve the effectiveness of the criminal justice system in NSW. The DPP is responsible for the prosecution of alleged NSW State offences of fraud against Comcare programs and systems.
<a href="#"><u>State Insurance Regulatory Authority (SIRA)</u></a>	SIRA is an independent government owned statutory body responsible for managing state-based accident insurance claims for all employer's without Comcare cover or a self-insurance licence.



<b>ACT</b>	
<a href="#">Australian Federal Police (AFP) – ACT Policing</a>	The AFP enforces ACT criminal law. The AFP is the lead agency in the investigation of ACT fraud against Comcare programs and systems.
<a href="#">ACT Office of the Director of Public Prosecutions (DPP)</a>	The ACT Office of the DPP is an independent body responsible for instituting, conducting and supervising criminal and related proceedings in courts in the ACT. The ACT DPP is responsible for the prosecution of alleged ACT offences of fraud against Comcare programs and systems.
<a href="#">WorkSafe ACT</a>	WorkSafe ACT is an independent government owned statutory body responsible for managing state-based accident insurance claims for all employer's without Comcare cover or a self-insurance licence.
<b>Victoria</b>	
<a href="#">Victoria Police (VICPOL)</a>	VICPOL provides a 24-hour police service to the Victorian community. VICPOL is the lead agency in the investigation of Victoria State offences of fraud against Comcare programs and systems.
<a href="#">The Victorian Office of Public Prosecutions (OPP)</a>	The Office of Public Prosecutions prepares and conducts criminal prosecutions on behalf of the Director of Public Prosecutions. The Victorian DPP is responsible for the prosecution of alleged Victoria State offences of fraud against Comcare programs and systems.
<a href="#">WorkSafe Victoria</a>	WorkSafe Victoria is an independent government owned statutory body responsible for managing state-based accident insurance claims for all employer's without Comcare cover or a self-insurance licence.
<b>Tasmania</b>	
<a href="#">Tasmania Police (TASPOL)</a>	TASPOL is the lead agency in the investigation of Tasmanian State offences of fraud against Comcare programs and systems.
<a href="#">Tasmania Director of Public Prosecutions (DPP)</a>	The Tasmania DPP provides an independent prosecution service to the state of Tasmania. The DPP is responsible for the prosecution of alleged Tasmanian State offences of fraud against Comcare programs and systems.
<a href="#">WorkSafe Tasmania</a>	WorkSafe Tasmania is an independent government owned statutory body responsible for managing state-based accident insurance claims for all employer's without Comcare cover or a self-insurance licence.
<b>South Australia</b>	
<a href="#">South Australian Police (SAPOL)</a>	SAPOL is the lead agency in the investigation of South Australian State offences of fraud against DSS programmes and systems.

<a href="#"><u>South Australian Office of the Director of Public Prosecutions (DPP)</u></a>	The Office of the DPP provides the people of South Australia with an independent and effective criminal prosecution service. The South Australian DPP is responsible for the prosecution of alleged South Australian State offences of fraud against Comcare programs and systems.
<a href="#"><u>Return To Work SA</u></a>	Return To Work SA is an independent government owned statutory body responsible for managing state-based accident insurance claims for all employer's without Comcare cover or a self-insurance licence.
<b>Western Australia</b>	
<a href="#"><u>Western Australian Police (WAPOL)</u></a>	In partnership with the community, the WAPOL create a safer and more secure Western Australia by providing quality police services. WAPOL is the lead agency in the investigation of Western Australian State offences of fraud against Comcare programs and systems.
<a href="#"><u>Western Australia Office of the Director of Public Prosecutions (DPP)</u></a>	The Office of the DPP is the independent prosecuting authority for the State of Western Australia, responsible for the prosecution of all serious offences committed against State criminal law. The Western Australian DPP is responsible for the prosecution of alleged Western Australian State offences of fraud against Comcare programs and systems.
<a href="#"><u>WorkCover WA</u></a>	WorkCover WA is an independent government owned statutory body responsible for managing state-based accident insurance claims for all employer's without Comcare cover or a self-insurance licence.
<b>Northern Territory</b>	
<a href="#"><u>Northern Territory Police (NTPOL)</u></a>	The Northern Territory Police, Fire and Emergency Services is referred to as a Tri-Service. The Tri-Service is responsible for the protection of life and property and the provision of disaster and emergency management to widely dispersed communities throughout the Northern Territory. The NTPOL is responsible for the prosecution of alleged Northern Territory offences of fraud against Comcare programs and systems.
<a href="#"><u>Northern Territory Office of the Director of Public Prosecutions (DPP)</u></a>	The Office of the DPP provides the people of the Northern Territory of Australia with an independent, professional and effective criminal prosecution service and is responsible for the prosecution of alleged Northern Territory offences of fraud against Comcare programs and systems.
<a href="#"><u>NT WorkSafe</u></a>	NT WorkSafe is an independent government owned statutory body responsible for managing state-based accident insurance claims for all employer's without Comcare cover or a self-insurance licence.

## **Risk Assessment and Prioritisation Model Policy**

The following Policy will be incorporated into the FIU *Fraud Investigations Manual*.

# **INITIATION AND CLOSURE OF FRAUD INVESTIGATIONS POLICY**

## **Policy Statement**

1. Pursuant to section 10(e) of the *Public Governance, Performance and Accountability Rule 2014 (fraud rule)*, Comcare is obliged to undertake investigations, or otherwise deal with incidents of, fraud or suspected fraud in relation to functions conferred on Comcare under any legislation.
2. This policy and the accompanying procedures, describe how Comcare will assess information reports and fraud referrals it receives (from any source) and recommend the initiation and closure of fraud investigations.
3. The key drivers for decisions are:
  - meeting obligations under the fraud rule; and
  - managing fraud risk in Comcare's areas of responsibility.
4. Comcare uses the assessment of risk to recommend and prioritise the investigation of fraud within its jurisdiction.
5. Comcare has documented processes detailing its decision-making processes and criteria for assessing, initiating and closing investigations.
6. These processes align with the Australian Government Investigation Standards 2022, Comcare's Compliance and Enforcement Policy and the CDPP Prosecution Policy and Guidelines.

## **Non-Compliance and Fraud**

### **Non-compliance**

7. *Non-compliance* means non-adherence with the rules, regulations and associated legislation relating to the schemes and business operations that Comcare administers.
8. Non-compliance can range from a simple mistake to criminal matters such as fraud. Non-compliance can be accidental or deliberate.
9. There are different types of non-compliance:
  - Error or mistake – a genuine mistake where there is no intention to gain something you are not entitled to.
  - Misuse – using benefits/funds in ways that are not consistent with entitlements.
  - Barely honest behaviour – practices that are not illegal but are unethical, unscrupulous or not in the interests of the general public.

- Criminal Fraud – intentionally (and knowingly) gaining a benefit or causing a loss or risk of causing a loss, through deceptive means.

10. Not all non-compliance is intentional and rises to the level of criminal fraud.

## Fraud

11. Fraud is a crime. It requires intent. People who commit fraud try to get benefits for themselves or others by being dishonest.

12. There are several ways people commit external fraud relating to Comcare. They include (but not limited to):

- providing false or misleading information;
- using fake documents and/or invoices;
- making claims for services or products that were not provided;
- misusing funds;
- unlawfully obtaining and/or using Comcare information or restricted data.

13. Comcare has zero tolerance for fraud and will always deal with instances of alleged fraud.

14. If someone unintentionally does the wrong thing, we consider this non-compliance.

## Voluntary Compliance

15. Comcare understands that the majority of its clients try to do the right thing but sometimes make mistakes.
16. Comcare wants to help those clients learn how to do the right thing before it escalates and becomes a more serious issue (e.g. incorrect entitlements are identified and debt recovery action is commenced).
  - o Clients include: injured workers, service providers, rehabilitation providers and Employers.
17. If clients make genuine mistakes or Comcare has inadvertently failed in its obligations, Comcare will work with relevant parties to fix the issue to generate voluntary compliance.

## Treatment Strategy

s 47E



## Information reports

### Origins

20. Reports of suspected fraudulent activities and/or non-compliance, known as *Information Reports* when received by FIU and *Non-Compliance Reports* when received by other Comcare business areas, may be received from a range of sources, including:

- Members of the public
- Service providers
- Comcare employees
- Other Commonwealth or State/Territory agencies
- Employers
- Government or ministerial referrals
- Scheduled auditing processes
- Integrity or compliance processes
- Intelligence activity.

### Information Report Receipt

#### *Fraud Investigations Unit*

21. Information reports are most commonly received through:

- Online “Reporting Fraud” form on [www.comcare.gov.au](http://www.comcare.gov.au) (received through the Fraud Inbox)
- A dedicated 1300 366 979 telephone number
- Comcare fraud inbox ([fraud@comcare.gov.au](mailto:fraud@comcare.gov.au))

22. All emails sent to [fraud@comcare.gov.au](mailto:fraud@comcare.gov.au) are received through the Fraud Inbox which is managed by FIU.

23. Access to this shared mailbox should be limited to the Chief Finance Officer and FIU.

24. The Fraud Inbox provides a platform for reporting of fraud related allegations.

25. Any information reports received by FIU which relate to other Group operations (unless it’s related to corruption or staff misconduct), will be referred to the appropriate team in that Group<sup>1</sup>.

26. All non-compliance behaviour observed by any staff in Comcare, which meets the definition of fraud (see below) and where a reasonable suspicion exists, will be referred to FIU<sup>2</sup>.

47E(d)

---

<sup>1</sup> For example, allegations related to injured workers or service providers will be referred to the Claims Compliance & Assurance Team; allegations relating to rehabilitation providers will be referred to the Workplace Rehabilitation Providers Performance Team.

<sup>2</sup> To be reasonably suspected of fraud: there must be more than mere suspicion, there must be some objective basis for the belief; the allegation must be judged as ‘somewhat reliable’. To be judged somewhat reliable, there must be corroborating information.

## Definition of 'Fraud'

28. Fraud is defined as:

‘dishonestly obtaining a benefit or causing a loss by deception or other means’<sup>3</sup>

29. This definition is based on the fraudulent conduct offences under part 7.3 of the *Criminal Code Act 1995* (Cth) (Criminal Code), other relevant offences under chapter 7 of the Criminal Code and the Commonwealth Fraud Control Framework 2017.

30. The following table can be used to guide judgements about whether the allegation meets the definition:

(i) Has there been a deception (lie or false representation) <sup>4</sup> ?	Yes – continue to (ii)	No – there is no fraud
(ii) Was the deception dishonest <sup>5</sup> in nature?  - Are there indicators that the perpetrator knew of the deception or had the intention to deceive?  - Knowledge can be inferred by an assessment of the perpetrator’s actions and/or admissions (e.g. telephone calls or emails)	Yes – continue to (iii)	No – there is no fraud
(iii) Did the deception <u>result</u> (or could have resulted) in obtaining benefits they would not have otherwise been entitled to?  - Alternatively, did the deception cause a loss (or could have caused a loss) which would not have otherwise occurred?  - Is the deception material to the benefit obtained?	Yes – likely to meet the definition of a ‘fraud’	No – there is no fraud

---

<sup>3</sup> includes ‘risk of loss’.

<sup>4</sup> An ‘omission’ to do something may also constitute a fraud however there should also be indicators that the perpetrator had knowledge (or should have known) of their obligations to act.

<sup>5</sup> Section 130.3 of the Criminal Code defines “dishonest” as: (a) dishonest according to the standards of ordinary people; and (b) known by the defendant to be dishonest according to the standards of ordinary people.

## Reasonable Suspicion

31. Once it is assessed that the allegation meets the definition of a fraud, the reliability and credibility of the allegation must be assessed to determine if there is 'reasonable suspicion' present.
32. To have reasonable suspicion, there must be more than mere suspicion, there must be some objective basis for the belief. The allegation must be judged as 'reliable' and 'credible'. This is a subjective assessment.<sup>6</sup>

## Fraud Referrals and the RAPT

33. Any fraud allegation which:

- o is Comcare-related;
- o meets the definition of fraud, and
- o is reasonably suspected of being true,

will be referred to the FIU via the Fraud Referral Form for further assessment.

s 47E(d)

## Records Management

39. All Information Reports and Fraud Referrals will be recorded in the FIU electronic case management system.

## Decision to initiate a fraud investigation

40. Comcare conducts fraud investigations to:

- o Ensure it is complying with its obligations under the fraud rule;
- o Provide specific and general deterrence against the defrauding of Comcare and its operations;
- o Maintain its reputation as an effective regulator and scheme administrator;

---

<sup>6</sup> Some useful questions to ask include - Is the allegation internally logical; Can the allegation be corroborated with other independent information; Is the informant normally reliable?

- Ensure its resources are not wasted, as a result of fraud and abuse.
- s 47E(d)

## **Decision to close a fraud investigation**

47. Closure of a fraud investigation can occur under the following circumstances:

- It becomes apparent that there is insufficient evidence to prove a criminal offence.
- During the conduct of the investigation, it appears that the information relied upon to recommend the commencement of a fraud investigation no longer exists (or has been found to be incorrect) and the situation is unlikely to change through the expenditure of further reasonable effort<sup>10</sup>.

---

<sup>7</sup> See Comcare Risk Management Procedure July 2022 - Attachment D – Risk appetite and tolerance.  
s 47E(d)

s 47E(d)





















