

Fraud Fusion Taskforce Terms of Reference

Dated: 22 May 2023

1. Purpose and scope

- 1.1. The Terms of Reference (ToR) for the Fraud Fusion Taskforce (this document) accompany the Fraud Fusion Taskforce Memorandum of Understanding (MOU) to establish the role, objectives and structure of the Fraud Fusion Taskforce, and how governance and administrative arrangements will operate for the Fraud Fusion Taskforce (the strategic framework).
- 1.2. Further, the ToR outlines the resources and financial plans to enable the Fraud Fusion Taskforce objectives to be achieved, provides a high-level schedule of the work to be undertaken, and a basis for future decision-making and planning among the key stakeholders.
- 1.3. The ToR commence on endorsement by the Fraud Fusion Taskforce Inter-Departmental Committee (IDC) following commencement of the MOU; and should be read in conjunction with the MOU.
- 1.4. The ToR is one of a suite of documents that underpin the establishment and operation of the Fraud Fusion Taskforce. Other documents and frameworks that will set out the requirements for how the Fraud Fusion Taskforce will operate are expected to include:
 - 1.4.1. MOU
 - 1.4.2. Fraud Fusion Taskforce Placemat
 - 1.4.3. Terms of reference for IDC and other committees
 - 1.4.4. Ethics & Human Oversight Framework
 - 1.4.5. Resourcing, Risk Management, MERI and Assurance Frameworks
 - 1.4.6. Communications Plan
 - 1.4.7. Data Governance Plan
 - 1.4.8. Savings Capture Plan
 - 1.4.9. Fraud Fusion Taskforce (Operational) Delivery Plan and Project Schedule
 - 1.4.10. Operational procedures and work plans.
- 1.5. The ToR will cease as at Close of Business 30 June 2026 unless extended by agreement of the Parties and in alignment with any MOU extension in accordance with clause 13 of the MOU.
- 1.6. Definitions of key terms, expressions and acronyms used in the ToR are provided in Annexure A.

2. Background

- 2.1. Fraud against Government programs is a long-standing issue for Government. Fraud is a significant risk for the NDIS and contributor to NDIS waste¹ (please refer further information under Current State in Annexure B). Critically, fraud also presents risks to the safety and wellbeing of people with disability who are participants in the NDIS, as a result of supports and services potentially not being provided and compromised service quality. It also presents a significant risk to the integrity and sustainability of the scheme.
- 2.2. The NDIA, in consultation with other Commonwealth agencies, has been considering how to enhance efforts to further protect and safeguard the NDIS against any deliberate and targeted criminal exploitation, particularly service provider fraud. Multi-agency collaboration has been identified as necessary to cohesively address fraud vulnerabilities in the NDIS and other government services, and address risks to participants.

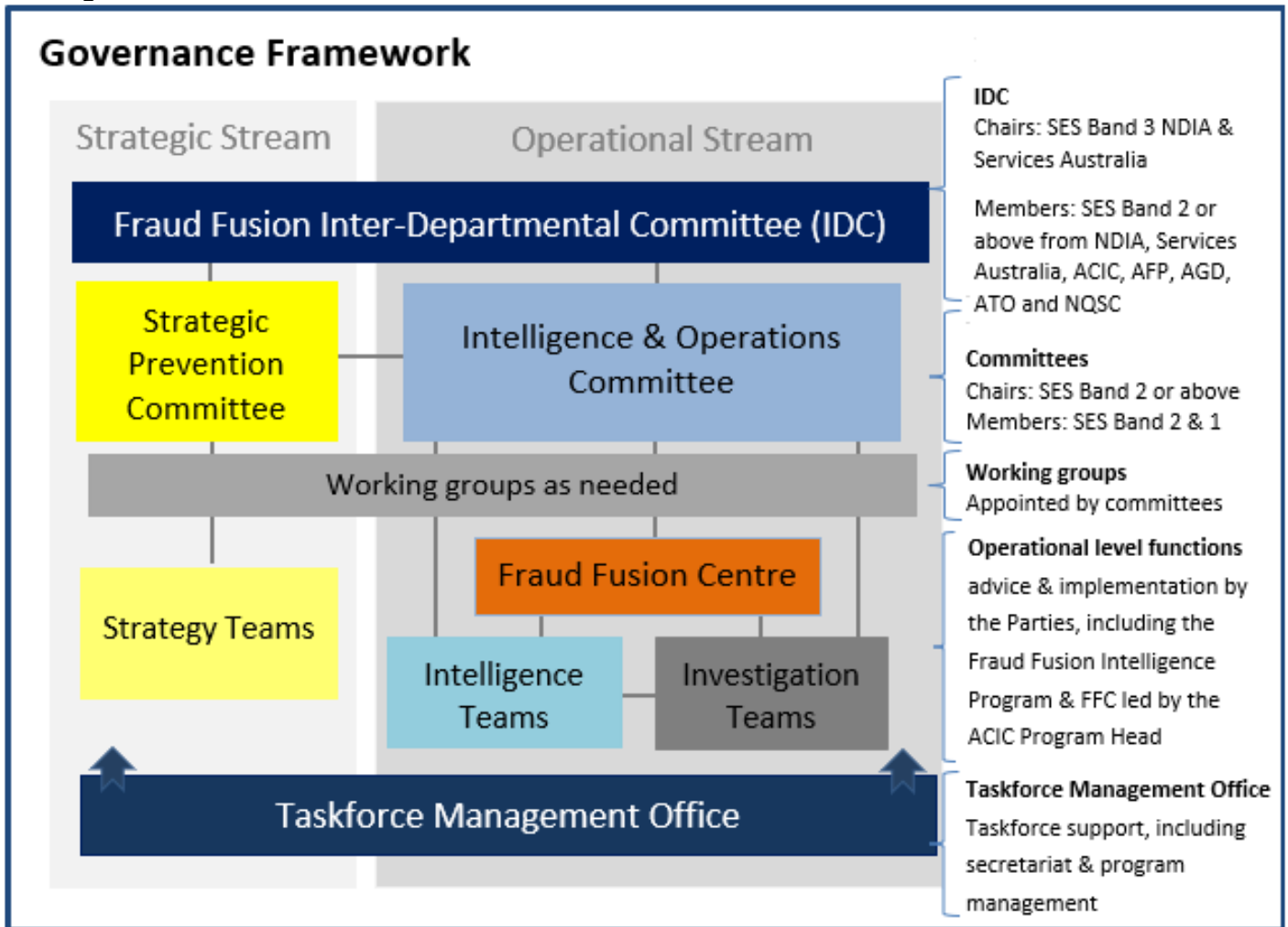
¹ Waste involves taxpayers not receiving reasonable value for money in connection with any government funded activities due to an inappropriate act or omission by an individual or entity with control over, or access to, government resources.

- 2.3. The Government made an election commitment to restore trust in the NDIS and ensure a better future for Australians living with a disability. The Minister announced in October 2022 that a multi-agency taskforce would be established to track down NDIS fraudsters.
- 2.4. The October 2022 budget confirmed funding of \$126.3m over four years from 2022-23 for the establishment of the Fraud Fusion Taskforce, with NDIA estimated savings offsets of \$291.5m recognised. DSS has also identified an additional \$11.4m of offsets, which will lead to a cost-neutral position for social security Taskforce Integrity for 2023-2024 after which funding ceases. The Fraud Fusion Taskforce replaces the NDIS Fraud Taskforce, and as part of the budget measure funding for Taskforce Integrity is extended until 30 June 2024 while it transitions into the Fraud Fusion Taskforce from 1 July 2023.
- 2.5. The current state, potential future state and expected benefits as well as funding arrangements are detailed in Annexure B.

3. Parties and Governance

- 3.1 The ToR is between the Parties, those agencies who agree to participate in the Fraud Fusion Taskforce and are signatories to the MOU (refer clause 17 of the MOU). The roles and responsibilities of specific Parties are outlined in the MOU.
- 3.2 Other agencies may join the Fraud Fusion Taskforce under subclause 13(4) of the MOU.
- 3.3 The governance structure for the Fraud Fusion Taskforce is outlined in Figure 1 below.
- 3.4 The Inter-Departmental Committee (IDC) will meet approximately six weekly and operate under the IDC Terms of Reference. It will report through agency heads to the Minister for the NDIS and Government Services. The IDC is responsible for strategic oversight and monitoring of the effective and efficient operation of the Fraud Fusion Taskforce and its performance against the deliverables. It will oversee and guide other Taskforce committees and provide advice to the Parties and Fraud Fusion Taskforce Officers in pursuit of the Fraud Fusion Taskforce objectives and deliverables to meet the Purpose of the Fraud Fusion Taskforce. The Deputy CEOs (ie. Senior Executive Service (SES) Band 3) of NDIA and Services Australia will Co-Chair the IDC. Membership will include NDIA, Services Australia, ACIC, NQSC, AGD, ATO and the AFP.
- 3.5 The Strategic Prevention Committee (SPC) will report to the IDC. It will meet approximately six weekly, or as required to meet IDC requirements, and operate under terms of reference established and approved by the IDC. The MOU states that it will be responsible for developing, implementing and supporting strategic preventative capability; and exploring and testing options that could form the basis of future advice to Government on a scalable assurance and prevention model that could increase payment and provider integrity across other government programs. SES Band 2 or above from the Parties will Co-Chair the SPC. The SPC Co-chairs will attend the IDC as observers if not already members.
- 3.6 The Intelligence and Operations Committee (IOC) will report to the IDC. This committee will also meet approximately six weekly, or as required to meet IDC requirements, and operate under terms of reference established and approved by the IDC. Its purpose is to oversee Fraud Fusion Taskforce operations and intelligence matters to ensure the objectives of the Fraud Fusion Taskforce are met, including achievement of savings targets. SES Band 2 or above from the Parties will Co-Chair the IOC. The IOC Co-Chairs will attend the IDC as observers if not already members. The Program Head for the Fraud Fusion Intelligence Program and the Fraud Fusion Centre is invited to attend and engage with the IOC as a member.
- 3.7 The IDC, SPC and IOC may appoint working groups to assist committees with their functions.
- 3.8 The Taskforce Management Office will provide governance, reporting, administrative, communications and program management support for the Fraud Fusion Taskforce. It will be resourced by the NDIA and incorporate teams responsible to support the Fraud Fusion Taskforce committees, including a secretariat function, and will be the central repository for governance information.

Figure 1 – Fraud Fusion Taskforce Governance Structure



4. Fraud Fusion Taskforce Purpose and Key Principles

The purpose of the Fraud Fusion Taskforce is outlined in the MOU as follows:

The purpose of the Fraud Fusion Taskforce is to improve payment integrity in government programs and payments by preventing or reducing fraud and criminal activity within and against government programs (including Serious and Organised Crime (SOC) and systemic fraud), to:

- a) *protect the safety and wellbeing of participants who are at risk of harm as a result of fraud, and related service quality.*
- b) *protect public finances and prevent or reduce financial losses.*
- c) *ensure appropriate use of funds and the sustainability of the programs.*
- d) *improve community confidence in the administration of those payments and programs.*

The Fraud Fusion Taskforce will have a:

- a) *Strategy focus:*
 - i. *developing, implementing and supporting strategic preventative capability*
 - ii. *exploring and testing options that could form the basis of future advice to Government on a scalable assurance and prevention model that could increase payment and provider integrity across government programs.*

- iii. *well-informed cross-program actions to help prevent fraud, by drawing on the capabilities and powers of the Parties.*
- b) *Intelligence and operational focus:*
 - i. *enhanced data and intelligence sharing, and intelligence development*
 - ii. *a coordinated government approach to detection and treatment of serious and organised crime offending against government programs and systemic fraud.*

The Fraud Fusion Taskforce will have a particular focus on the NDIS, initially, with broader fraud and loss detection and prevention benefits for other government programs to follow. Taskforce Integrity will transition into the Fraud Fusion Taskforce from 1 July 2023 and be under the Fraud Fusion Taskforce remit from this date. The Fraud Fusion Taskforce will enable intelligence sharing, identification and response by the Parties to identify and address fraud perpetrated by SOC entities and others seeking to exploit the Government's programs.

This Fraud Fusion Taskforce purpose is further defined in purpose statements within in the MOU:

The Fraud Fusion Taskforce will:

- a) *Identify, understand, prevent, respond to and disrupt fraud and criminal activity against the NDIS and other government programs, particularly SOC and systemic fraud, by:*
 - i. *sharing data and information in order to improve integrity through analysing data to identify potential fraud and associated behaviours affecting government payments and programs.*
 - ii. *identifying, developing and coordinating preventative and treatment strategies domestically and internationally.*
- b) *Protect participant safety, service quality and the public finances of Australia, and improve payment integrity, by combatting fraud and criminal activity, including SOC and systemic fraud, against the NDIS and other government programs and payments.*
- c) *Enhance government coordination to prevent, detect and respond to fraud and related criminal activity within and against government programs, including SOC and systemic fraud, and improve integrity, including by:*
 - i. *reconciling government payments to identify fraudulent transactions (such as the application of duplicate claims indicating fraudulent claims).*
 - ii. *collecting, correlating, analysing and disseminating information and intelligence to develop appropriate responses to criminal activity and fraud, including SOC.*
 - iii. *processing new intelligence insights through multi-agency data and information sharing under the Fraud Fusion Intelligence Program, by the Fraud Fusion Centre and between the Parties and Fraud Fusion Taskforce Officers.*
 - iv. *developing capability to support a single view of entities and individuals that may be or are confirmed to be committing fraud and associated criminal activity, including SOC, in order to address associated risks.*
 - v. *enhancing and maturing the management of cases requiring active intervention, including developing different layers of case treatment and intervention.*
- d) *Generate and use intelligence insights to inform preventative and systemic control enhancements and further investment opportunities, drawing on the capabilities and powers of relevant agencies, including through:*

- i. *the identification of system vulnerabilities.*
 - ii. *cross program actions.*
 - iii. *targeted treatment to prevent fraud and criminal activity and improve integrity in Government programs (including targeting SOC and systemic fraud).*
- e) *Prepare advice for Government as appropriate on a scalable assurance and prevention model that could increase payment and provider integrity across other government programs.*

Note 1: *Each Party will contribute to these purposes to the extent of their legislative framework and any conditions imposed on their involvement in the Fraud Fusion Taskforce per subclause 13(4)(a).*

The key principles for the Fraud Fusion Taskforce are stated in the MOU:

1. *The Fraud Fusion Taskforce operates as a multi-agency Taskforce, working together to disrupt fraud and criminal activity, including SOC, and improve integrity, with the Parties recognising each other's respective roles and responsibilities in supporting their own relevant program and payment administration, intelligence, investigation and treatment processes.*
2. *The Parties will be operationally independent, but to the furthest extent possible, will engage in close cooperation and consultation, and ensure those employed to work on activity under the Fraud Fusion Taskforce (Taskforce Officers), achieve efficient and effective outcomes from both an individual agency and across government perspective in accordance with the Fraud Fusion Taskforce purpose clause 5.*
3. *The Fraud Fusion Taskforce will uphold the safety, security and wellbeing of participants of the NDIS and customers of other government programs and payments as its highest priority. The Fraud Fusion Taskforce will have primary regard to any risks arising for participants and customers when considering relevant and appropriate treatment options for matters in relation to alleged or confirmed fraud.*
4. *The Fraud Fusion Taskforce will be underpinned by a rigorous Ethics & Human Oversight Framework, to be endorsed by the IDC, and will have human oversight of all decision logic, governance controls and treatment approaches determined by the Fraud Fusion Taskforce.*

5. Vision, Objectives and Measures of Success

5.1 Fraud Fusion Taskforce vision

- a) *NDIS and other government programs have enhanced resilience to fraud and SOC. There is reduction in opportunity for commission of fraud and non-compliance as well as reduced incidents and financial losses, and enhanced government and community confidence due to improved program integrity.*

5.2 Fraud Fusion Taskforce immediate objectives:

- b) *Enhanced government coordination of fraud detection, response, investigation and prevention with a SOC focus, including by:*
 - i. *reconciling government payments across Government entities.*
 - ii. *processing new and enhanced intelligence insights.*
 - iii. *developing a single view of entities and individual fraud and payment integrity risks through multi-agency data and information sharing.*
- c) *Inform preventative and systemic control enhancements and further investment opportunities, including through cross-program actions and targeted treatment to prevent fraud, by drawing on the capabilities and powers of relevant agencies.*

- d) Coordinate regulation and treatment in relation to fraud, non-compliant activity and payment error with SOC focus.

5.3 Fraud Fusion Taskforce longer term strategic objectives:

- a) The Commonwealth can effectively identify, respond to and take action to address criminal activity, including SOC, which presents the highest fraud risks to the NDIS and other government programs and payments and risks to the safety and wellbeing of participants.
- b) Reduced vulnerability to SOC in the NDIS and other government programs, and for genuine participants of these programs.
- c) The Fraud Fusion Taskforce has disrupted and prosecuted perpetrators and enablers of fraud and serious crimes against the NDIS and other government programs.
- d) Strategic prevention options have been explored and tested through the Fraud Fusion Taskforce that contribute to a scalable assurance and prevention model that increases payment and provider integrity across other government programs.
- e) The community has confidence in the Fraud Fusion Taskforce and the integrity of the NDIS and other government programs.

5.4 Measures of success:

- a) Success of the Fraud Fusion Taskforce is expected to be determined based on the following key measures of success; these and other measures will be addressed in the Fraud Fusion Taskforce MERI Framework:
 - i. reduction in risk and harm to individuals receiving supports and services.
 - ii. value of prevented fraud through improved controls and earlier detection.
 - iii. number of identified cases through data sharing and analytics.
 - iv. number of matters referred to the CDPP and prosecuted.
 - v. number of fraud cases identified and successfully disrupted.
 - vi. total value of fraud under investigation.
 - vii. total Commonwealth funds returned through criminal and administrative recovery.
 - viii. number of regulatory outcomes including banning and suspension orders.
 - ix. number of strategic intelligence insights and briefings identifying impact of fraud and loss leading systemic, administrative and other interventions.
- b) Fraud Fusion Taskforce performance and outcomes will be formally evaluated and reported to the responsible Minister and senior stakeholders at agreed times during the program as outlined in the agreed comebacks.
- c) The Fraud Fusion Taskforce will also be subject to continuous evaluation and improvement as well as routine management reporting, addressed in the MERI Framework.

6. Deliverables

- 6.1 Stream A: **Strategy and Prevention Activity** – overseen by the Strategic Prevention Committee (SPC): Deliver on the responsibilities and functions outlined in the SPC Terms of Reference (SPC ToR) and approved by the IDC, and the strategic aspects of the purpose and objectives outlined in clauses 4 and 5.
- 6.2 Stream B: **Fraud Fusion Taskforce Operations Activity** – overseen by the Intelligence and Operations Committee (IOC): Deliver on the responsibilities and functions outlined in the IOC Terms of Reference (IOC ToR) and approved by the IDC, and the operational and intelligence aspects of the purpose and objectives outlined in clauses 4 and 5.

- 6.3 **Taskforce Integrity:** Taskforce Integrity activity under the lead of Services Australia will be transitioned into the Fraud Fusion Taskforce during 2023-24, in accordance with a transition plan to be endorsed by the IDC.

7. Roles and Responsibilities

- 7.1 The Parties will actively assist each other and collaborate to meet the Fraud Fusion Taskforce purpose and objectives referred in the MOU and in clauses 4 and 5 of this ToR in accordance with the roles and responsibilities and services outlined in the MOU and Annexure C.
- 7.2 The ACIC, responsible for the Fraud Fusion Centre and the Fraud Fusion Intelligence Program, agrees to provide criminal intelligence to support the strategic purpose and objectives of the Fraud Fusion Taskforce.
- 7.3 The Parties are responsible for delivering on the Government commitments (including the offsets, as appropriate to each Party's functions and responsibilities) under the October 2022 budget measure *Fraud Fusion Taskforce* – as outlined in Annexure B.
- 7.4 Services Australia is responsible for delivering on the Government commitments that effect a cost-neutral status for Taskforce Integrity, under the October 2022 budget measure Fraud Fusion Taskforce as outlined in Annexure B.

8. Data Sharing

- 8.1 Data sharing arrangements are outlined in the MOU and the Data Governance Plan
- 8.2 Specific programs and payments that are the subject of Fraud Fusion Taskforce activity and any additional data-sharing protocols and prioritisation are outlined in Annexure D.

9. Key Contacts

The key contact who will administer this ToR

Secretariat, Taskforce Management Office (TMO): fraudfusiontaskforce@ndis.gov.au

⁵ Subdivision 355-B of Schedule 1 to the *Taxation Administration Act 1953* (Cth)

⁶ A *taskforce officer* is defined in subsection 355-70(11) of Schedule 1 to the *Taxation Administration Act 1953* (Cth)

⁷ Subsection 355-70(1) table item 4 of Schedule 1 to the *Taxation Administration Act 1953* (Cth)

⁸ Section 355-30 of Schedule 1 to the *Taxation Administration Act 1953* (Cth)

⁹ Section 355-175 of Schedule 1 to the *Taxation Administration Act 1953* (Cth)

Annexure A - Definitions

The following words, expressions and acronyms have the following meanings in this ToR unless a contrary intention appears:

Words and expressions	Meaning
ACC Act	<i>Australian Crime Commission Act 2002 (Cth)</i>
Accountable Authority	The agency head, within the meaning given by section 7 of the Public Service Act 1999
ACIC	Australian Criminal Intelligence Commission, the name the Australian Crime Commission operates under as permitted by the ACC Act and the <i>Australian Crime Commission Regulations 2018 (Cth)</i>
AFP	Australian Federal Police
AGD	Attorney-General's Department
Annexure	An annexure to this ToR
ASIC	Australian Securities and Investments Commission
Assurance Framework	A structured means of identifying and mapping the main sources of assurance for the Fraud Fusion Taskforce and coordinating these to address the purpose and objectives of the Fraud Fusion Taskforce
ATO	Australian Taxation Office
AUSTRAC	Australian Transaction Reports and Analysis Centre
CDPP	Commonwealth Director of Public Prosecutions
CEO	Chief Executive Officer
Close of Business	5.00PM Australian Eastern Standard Time
Communications Plan	Outlines key stakeholder communications and engagement arrangements for the Fraud Fusion Taskforce
Criminal activity	Criminal activity means a criminal offence under a law of the Commonwealth, a State or a Territory, of Australia.
Data Governance Plan	Documented data sharing and security framework for the Fraud Fusion Taskforce
DEWR	Department of Employment & Workplace Relations
DoE	Department of Education
DoHA	Department of Health and Aged Care
DSS	Department of Social Services
DVA	Department of Veterans' Affairs

Fraud	Dishonestly obtaining a benefit, or causing a loss, by deception or other means. (Note: This is intentional action on the part of the offender)
Fraud Fusion Centre	Managed by the ACIC under an ACIC Program Head – this will operate as the centralised mechanism to enable data acquisition, detection analytics and the identification of opportunities for information-sharing. It will be staffed with Fraud Fusion Taskforce Officers from some of the Parties who will be engaged by the ACIC as ACIC members of staff under the ACC Act
Fraud Fusion Intelligence Program	Managed by the ACIC under an ACIC Program Head - Program involving the ACIC collecting criminal intelligence and analysing and crossmatching data from numerous sources (including but not limited to the NDIA, Services Australia, NQSC, ATO, AFP, ASIC, AUSTRAC, DoHA, DoE and DEWR) to provide strategic and tactical intelligence advice to the Fraud Fusion Taskforce and its members to address the purpose and objectives of the Fraud Fusion Taskforce
Fraud Fusion Taskforce Officer (Taskforce Officer)	A person holding an office in, employed in performing services for any of the Parties and engaged to work on strategic or operational activity of the Fraud Fusion Taskforce; this person is required to act to meet the purpose of the Fraud Fusion Taskforce as set out in clause 5. A Taskforce Officer for ATO disclosure purposes is defined in subsection 355-70(11) of Schedule 1 to the <i>Taxation Administration Act 1953</i> (Cth).
Fraud Fusion Taskforce Risk Management	Strategic, operational and integrated risk management practices, including integration with governance practices, decision-making and assurance processes of the Fraud Fusion Taskforce, having appropriate regard to risk management standards and government policy
GST	Has the same meaning as given in the <i>A New Tax System (Goods and Services Tax) Act 1999</i> (Cth)
IDC	Fraud Fusion Taskforce Inter-Departmental Committee
Loss / Waste	Taxpayer / Government money or equivalent value stolen, paid and/or lost due to activity not supported by the governing regulatory framework for a government program
MERI Framework Monitoring, Evaluation, Reporting and Improvement Framework	Overarching framework for evaluation and reporting in relation to the Fraud Fusion Taskforce that includes performance monitoring and improving the approach of the Fraud Fusion Taskforce to most effectively manage serious and organised fraud in the NDIS and other government support programs

MOU	Memorandum of Understanding for the Fraud Fusion Taskforce
MYEFO	Mid-Year Economic and Fiscal Outlook process
NDIA	National Disability Insurance Agency
NDIS	National Disability Insurance Scheme
NDIS Act	<i>National Disability Insurance Scheme Act 2013</i> (Cth)
Non-compliance / Non-compliant	Refers to both intentional non-compliant acts (fraud) and unintentional non-compliant acts (error). The primary focus of the Fraud Fusion Taskforce is on fraud that relates to SOC and/or criminal activity which is established through consideration of non-compliance
NQSC	NDIS Quality and Safeguards Commission
Participant	A person who is the intended recipient of support under a government program / a related payment/s as determined by the relevant legislation and government policy (may be termed 'customer' in relation to some programs and payments).
Parties	Agencies who agree to participate in the Fraud Fusion Taskforce and are signatories to the MOU (MOU clause 17), as amended from time to time
Payment	An amount paid or payable (or the action or process of paying) to a recipient in respect of a government program that falls under the scope of the Fraud Fusion Taskforce
Payment Integrity	Ensuring payments are valid and correct in all respects, including being compliant with the legislation, paid to the appropriate person, in the correct amount and received by the intended person in a timely manner
Public Interest Certificate (PIC) – plural used: PICs	Public Interest Certificate or Authorisation – an authorisation for the disclosure of protected agency information if it meets the purposes set out in the governing legislative instrument (e.g., NDIS Act). A PIC comprehensively outlines the intended purpose of disclosure so a delegate of the CEO or other Accountable Authority of the agency can make an informed decision whether to disclose or not.
Privacy Impact Assessment (PIA)	A systematic assessment that identifies the impact that a project might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact.
PSPF	Australian Government Protective Security Policy Framework- refer https://www.protectivesecurity.gov.au

Resourcing Framework	The arrangements for resourcing the Fraud Fusion Taskforce, addressing the relevant budget measure for the Fraud Fusion Taskforce
Risk Management Framework	Fraud Fusion Taskforce Risk Management Framework setting out how the Fraud Fusion Taskforce approaches risk management and how risk management practices are integrated with governance practices, decision-making and assurance processes of the Fraud Fusion Taskforce, having appropriate regard to risk management standards and government policy
Savings Capture Plan	Savings Recognition and Capture Plan - provides an overview of how specific savings (including budget measure offsets) will be recognised and captured in respect of the Fraud Fusion Taskforce
Serious and organised crime (SOC)	Has the same meaning as 'serious and organised crime' given under the ACC Act
Systemic fraud	Fraud that is commonplace / widespread and is at a significant scale and risk impact to the NDIS or other government program and involves organised offending.
Taskforce Integrity	Joint operation between Services Australia and the AFP to prevent, detect and disrupt serious fraud and identity crime, within the Government's system of social supports
Taskforce Management Office	Fraud Fusion Taskforce Management Office - Teams responsible to support the Fraud Fusion Taskforce committees that provide structured governance and project management oversight (including creation of a staged Project Management Plan), secretariat and communications functions, as well as acting as the central repository for information on projects of the Fraud Fusion Taskforce (also known as the TMO).
Treatment	One or more options for addressing a fraud and any related fraud risk.

Annexure B - Background

Current State

- 1) The NDIA operates in a complex environment, supporting some of the most vulnerable in our society under the NDIS, which makes the Scheme a very attractive target for fraudulent activities and organised crime. The NDIA has seen an extensive increase in participants from 29,716 in 2016 to over 534,600 as of 30 June 2022. s 47E(d)
- 2) The NDIS Quality and Safeguards Commission, the regulator of NDIS providers and persons involved with NDIS support and service delivery, similarly operates in this complex environment. The Commission commenced in July 2018 and became fully operational nationally in December 2020. s 47E(d)
- 3) The NDIS could be considered a 'high risk'² program for target by fraud offenders, including serious and organised crime entities s 47E(d)
- 4) Organised criminals have been found to have created reusable business models to take advantage of the NDIS and a broad range of government programs. In some cases, this has included horizontal and vertical integration across programs and jurisdictions. The incidence of fraud offenders defrauding both NDIS and other government programs has become evident.
- 5) There are a number of fraud and integrity measures across government including the activities of the Commonwealth Fraud Prevention Centre (CFPC) within the Australian Government Attorney-General's Department and other measures deployed by NDIA, Australian Federal Police (AFP), Services Australia and other Commonwealth programs. These are further addressed under the section, 'Future State' below.
- 6) The NDIS has seen significant increase in fraud risk and targeting by criminals and opportunists. This is aligned with the history of Australian Government programs being accessed inappropriately by entities or individuals. Over time this has created:
 - Risk to participants, their safety and wellbeing.
 - Risk to program payments from fraud and similar divergent behaviour.
 - Reputational risk.
 - Growth industry which has allowed some controlling minds and interests to develop reusable business models to take advantage of a broad range of government programs. In some cases, this has included horizontal and vertical integration across programs and jurisdictions.
 - Significant cost in reacting to these challenges will remain high if more proactive measures are not implemented.
 - Increased program outlay and lost revenue

² Internationally, programs are often considered 'high risk' as a result of significant and inherent vulnerabilities to fraud, waste and abuse (US example: [High-Risk Series: Key Practices to Successfully Address High-Risk Areas and Remove Them from the List | U.S. GAO](#), UK example: .

- 7) The NDIA and agency partners have clear intelligence and evidence obtained over recent years that the NDIS and other Commonwealth programs are being targeted by serious and organised crime entities (SOC)³. s 47E(d)
- 8) A precise estimate of loss in the NDIS is not yet known because of a lack of data (this is a key issue the Fraud Fusion Taskforce seeks to remedy). International comparators based on United Kingdom research suggest losses due to fraud, non-compliance and incorrect payments of up to 10 per cent in 'high risk' programs.
- 9) A report commissioned by the Attorney-General's Department in 2019, estimated the cost of reported and unreported fraud and error against the Commonwealth is likely to be between 3 - 5.95% of government revenue.⁴

In the case of the NDIS, losses of 5.95% would have equated to over \$1.7 billion in 2021-22 (or 10% to over \$2.87 billion). Without appropriate investment, this would be expected to increase as the Scheme outlays continue to grow to support Australians with disability.
- 10) Examples of divergent behaviour by providers, i.e., their failure to meet obligations whilst participating in the NDIS are outlined in the diagram below.
- 11) s 47E(d)
- 12) s 47E(d)

³ Refer Guide developed in collaboration with Deloitte by the Commonwealth Fraud Prevention Centre [Counter Fraud Investment Cases Leading Practice Guide](#), including pg. 19. Also refer: [NDIS taskforce to hunt down organised crime groups 'robbing' billions from disability clients - ABC News](#) and [NDIS fraud reports reveal the scheme's weakest points \(theconversation.com\)](#)

⁴ Please refer report [Counter Fraud Investment Cases Leading Practice Guide](#) pg. 8.

Current state

Divergent Capabilities – limit the capability and capacity for verification, validation and fraud detection.



s 47E(d)

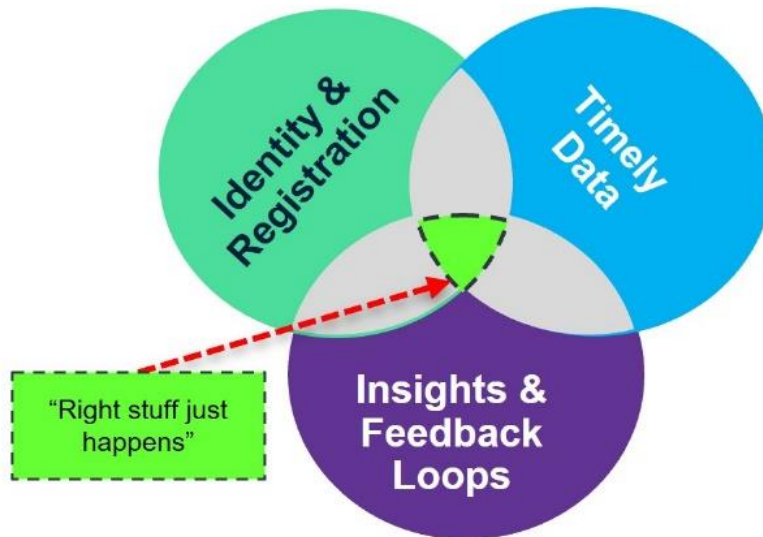
Future State and Expected Benefits

- 1) The Fraud Fusion Taskforce will complement and enhance existing Australian Government measures by enabling improved cross-program data and information-sharing, and strategic analysis of this data to identify fraud and examine the operation of serious, organised crime perpetrators. This will mean that datasets currently held discretely by individual Government entities can be aligned to strengthen evidence for supports and to verify the identity of those participating in the NDIS and other government programs.
- 2) The Fraud Fusion Taskforce will facilitate enhanced government collaboration in respect of fraud intelligence and treatment for the NDIS and other government programs. Operations will be coordinated between the partnering agencies to take well-informed and effective action against individuals and entities involved in the commission of fraud against Commonwealth programs. The agencies will be able to identify and confirm threat risks and models and systemic loss more broadly to government to take more effective, targeted action to prevent fraud and recover losses.
- 3) The future state that the Fraud Fusion Taskforce seeks to achieve is a sophisticated data-informed and enhanced government capability to detect and respond effectively to fraud across government programs, with a key focus on the NDIS and welfare supports under Taskforce Integrity. Partner agencies will provide data and share intelligence with the Fraud Fusion Taskforce and will benefit from the strategic insights and the coordinated action against fraud enabled through the Fraud Fusion Taskforce's function. The public benefit to be realised from operations of the Fraud Fusion Taskforce is expected to be substantial, including significant reduced loss of public funds that will, therefore, reach their intended use and recipient base.
- 4) Key benefits expected are:
 - Capability uplift – enhanced data acquisition, sharing, detection analytics and treatment across government.
 - Reduced risks to participants of the NDIS and other programs including reduced loss to fraud that can reduce available funding.
 - Improved service quality over time by supporting regulatory, legal and robust administrative action against serious and organised crime and systemic fraud.
 - Trust in the NDIS, other programs and Government.
 - Savings returned to Government and overall reduction in loss to NDIS and other government programs.
- 5) The Fraud Fusion Taskforce is also expected to contribute to the identification of a broader suite of potential debt and savings within each program managed by the partner agencies.
- 6) The Fraud Fusion Taskforce structure, supported by increased specialist technical capability and capacity in the NDIA, Services Australia and the NQSC, will identify, respond and better prevent fraud and loss and enable enhanced government coordination of detection and treatment responses to fraud as well as informing cross-program actions to help prevent fraud, drawing on the capabilities and powers of relevant agencies through Fraud Fusion Taskforce members (the Parties). This will enhance prevention of serious organised crime activity and the exploitation of Commonwealth payments and programs, including the movement of criminals between sectors and programs.

- 7) The Fraud Fusion Taskforce will achieve outcomes including fraud and loss reduction and enhanced integrity of the NDIS and other government programs through highly informed and targeted fraud detection, and investment in systemic controls and preventative measures. This will reduce opportunity for all types of fraud include serious and organised fraud and prevent loss of funds currently going to criminal individuals and entities. Significant outcomes include reduction of the personal and financial impact on victims of fraud both in the NDIS and in other government programs through shared data, information and capability.
- 8) The Fraud Fusion Taskforce will inform and complement many existing fraud and integrity initiatives, or these will be merged within its scope as noted below.
- 9) It is expected that the Commonwealth Fraud Prevention Centre (CFPC) (oversighted by AGD) will continue to play an essential role as part of its existing remit to provide support to agencies to design fraud resistant policies and programs. Insights from the Fraud Fusion Taskforce will assist the CFPC to help agencies to identify areas of fraud risk and fraudulent behaviour to better target prevention efforts. The CFPC will also provide advice on the financial and non-financial benefits from fraud prevention-based activities to inform partner agencies, the NDIS and other government programs.
- 10) Taskforce Integrity activity will come under the remit of the Fraud Fusion Taskforce from 1 July 2023 and Services Australia has been resourced for continuing operations of Taskforce Integrity up to the end of 2023-24 and to finalise the transition into the Fraud Fusion Taskforce (under transitional funding arrangements). It should be noted that no operational response funding beyond 30 June 2024 has been secured for Taskforce Integrity and this is expected to be subject to a comeback in 2023 where appropriate. Taskforce Integrity is a joint taskforce between Services Australia and the AFP and is focused on specific fraud against social support payment programs (e.g., Centrelink and Medicare customer fraud). Merging the work program of Taskforce Integrity with the Fraud Fusion Taskforce will enable improved information sharing and better coordination to respond to individuals targeting Government payments. Funding arrangements have been proposed to ensure seamless transition will occur.
- 11) The Fraud Fusion Taskforce will replace the existing NDIS Fraud Taskforce, which is a partnership between NDIA, the AFP and Services Australia and has successfully served search warrants and resulted in fraud offender arrests, asset seizures and convictions s 47E(d)

Future state

Convergent Capability: increase capacity for verification, validation and fraud detection. **Non-compliant behaviours eliminated/reduced.**



Ethics & Human Oversight Framework

- Providers participating in the NDIS and other government programs are compliant and on level playing field
- Identity of providers, associates and staff is validated by government
- Provider data is contemporary and available to agencies as required
- Risk flags recognised, aligned and analysed across jurisdictional spaces
- Intelligence optimised on divergent behaviour and serious and organised crime
- New differentiated intelligence, prevention and treatment strategies
- Feedback loops enable preventative strategies across programs/jurisdictions
- Provider payments reported to ATO close to real-time
- Systemic approaches to improve integrity are underpinned by a robust Ethics and Human Oversight Framework

Funding and Payment Provisions

- 1) Funding for the establishment of the Fraud Fusion Taskforce provided to specific agencies in the October 2022 Budget is outlined in the table below (October 2022-23 Budget Measures Part 1 page 9).
- 2) The October 2022 Portfolio Budget Statements state the following on pages 18 & 126, about the measure:

A further \$126.3 million in funding over 4 years will establish a Fraud Fusion Taskforce with the cooperation of 14 agencies to strengthen fraud detection and better safeguard the NDIS from serious organised crime....

The Australian Government is committed to strengthening the Commonwealth's fraud detection and response capability across key government services, including the NDIS, Centrelink, and Medicare. The Australian Government will establish a Fraud Fusion Taskforce to better enable intelligence sharing, identification and response by the NDIA, Services Australia, law enforcement agencies and regulators to fraud perpetrated by serious organised crime entities and others seeking to exploit the government's system of social supports.

Agency funding \$	2022-23	2023-24	2024-25	2025-26
NDIA	10.4M	15.9M	16M	16.1M
Services Australia	1.6M	13.8M*	3.6M	4.7M
ACIC	1.2M	1.3M	1.3M	1.3M
NQSC	2.2M	4.9M	5.0M	5.0M
ATO	2.5M	3.0M	2.8M	2.8M
AFP	0.9M	1.3M	1.3M	1.3M
DEWR	0.5M	0.5M	0.5M	0.5M
DoE	0.3M	0.4M	0.4M	0.4M
ASIC	0.2M	0.9M	1.0M	1.0M
DVA	0.4M	0.6M	0.6M	0.6M
DSS	neutral cost position with savings			

*includes funding to extend Taskforce Integrity for an additional year in 2023-24

- 3) Funding beyond June 2026 will be subject to relevant consideration by Government based on agreed comebacks – information on comebacks will be provided separately to committee members as appropriate.
- 4) The offsets (estimated savings) required to be achieved October 2022 budget measure *Fraud Fusion Taskforce* are as follows:

Estimated (\$)	2022-23	2023-24	2024-25	2025-26	Total
Total debt recovery of fraudulent payments received by providers	45.9M	68.8M	68.8M	68.8M	252.3M
Total debt recovery of serious non-compliant payments received by providers	7.1M	10.7M	10.7M	10.7M	39.2M
Total	53M	79.5M	79.5M	79.5M	291.5M

- 5) Services Australia is responsible for delivering on the following Government commitments that effect a cost-neutral status for Taskforce Integrity, under the October 2022 budget measure *Fraud Fusion Taskforce*:

\$	2023-24	2024-25	2025-26	Total
Saving offset	6.5M	2.8M	2.2M	11.4M

Annexure C

Clarified/Additional Agency Services

Additional Service Information	Description / Details
None currently	

Annexure D
Programs and Payments

Focus on prioritisation of programs and payments for Fraud Fusion Taskforce

Program / Payment	Details
NDIS	National Disability Insurance Scheme – first priority focus for Fraud Fusion Taskforce

Inter-Departmental Committee Terms of Reference

Fraud Fusion Taskforce

Dated: 22 May 2023

Inter-Departmental Committee Terms of Reference

Fraud Fusion Taskforce

1. Background

- 1.1 The Fraud Fusion Taskforce has been formed to strengthen the Commonwealth's fraud detection, prevention and response capability through enhanced data-sharing and intelligence, a coordinated government approach to detection and treatment of serious and organised crime and systemic fraud, and well-informed cross-program actions to help prevent fraud. This will draw on the capabilities and powers of the agencies that are Parties to the Memorandum of Understanding for the Fraud Fusion Taskforce (MOU).
- 1.2 The Fraud Fusion Taskforce will develop multi-agency capability and an enhanced government intelligence base and create scalable solutions to prevent, detect and respond to fraud affecting the National Disability Insurance Scheme (NDIS) and other Australian government programs and payments, and Australians who are intended participants and recipients. This will result in reduced 'waste' due to fraud, non-compliance and incorrect payments and impacts for participants and intended stakeholders of such programs.
- 1.3 The MOU sets out the governance and responsibilities for the Inter-Departmental Committee (IDC) as follows:

A Fraud Fusion Taskforce Inter-Departmental Committee (IDC) will be co-chaired by Deputy CEOs of the NDIA and Services Australia (i.e., Senior Executive Service (SES) Band 3 members). The IDC will:

- a) *Operate under its own terms of reference.*
- b) *Have a membership of other representatives at SES Band 2 or above from NDIA, Services Australia, ACIC, AFP, AGD, ATO and NQSC, which will be responsible for:*
 - i. *providing strategic oversight and monitoring of the effective and efficient operation of the Fraud Fusion Taskforce and its performance against the deliverables*
 - ii. *overseeing and guiding other Taskforce committees (refer subclauses 7(4) and 7(6)) and providing advice to the Parties and Fraud Fusion Taskforce Officers in pursuit of the Fraud Fusion Taskforce objectives and deliverables, to meet the Purpose in clause 5.*

For the IDC, proxy representation is allowed at SES Band 2 or above, or by exception below SES Band 2 with the agreement of both Co-Chairs. The Co-Chairs can be proxy for each other; or if neither is available, they can assign a proxy of their choice.

 Fraud Fusion Taskforce – Inter-Departmental Committee Terms of Reference

In addition to the above, the table below outlines further responsibilities for the IDC as outlined in the MOU:

MOU Reference	Responsibility
Subclause 6(4)	Endorse the Ethics & Human Oversight Framework for the Fraud Fusion Taskforce
Subclause 7(11)(a)	Endorse the strategic framework for Fraud Fusion Taskforce as set out in the Fraud Fusion Taskforce ToR
Subclause 8(3)	Endorse the Fraud Fusion Taskforce Communication and Engagement Strategy
Subclause 9(1)	Endorse the Monitoring, Evaluation, Reporting and Improvement Framework (MERI Framework) developed under direction of the IDC for the Fraud Fusion Taskforce
Subclause 9(1)	Endorse the Risk Management Framework developed under direction of the IDC for the Fraud Fusion Taskforce
Subclause 9(4)	Decide in respect of which Party new intellectual property created by the Fraud Fusion Taskforce will vest
Clause 12	Manage matters under dispute as outlined in MOU
Subclause 14(1)	Endorse Fraud Fusion Taskforce Data Governance Plan
Subclause 14(11)	Receive information and report on a suspected Eligible Data Breach and direct any relevant action
Subclause 13(3)	Review of MOU Variations to MOU – endorsement prior to agreement by all Parties
Subclause 13(4)	Consulted about variation to the MOU including for a new Party and determination of membership conditions, prior to variation agreement from all Parties
Subclause 13(5)	Termination of MOU or notification in respect of a Party

- 1.4 Definitions of key terms, expressions and acronyms used in this IDC ToR are the same as defined in the Fraud Fusion Taskforce MOU and ToR.

2. Purpose

- 2.1 These Terms of Reference articulate the scope of work and arrangements for the IDC and how members will work together to meet the relevant terms of the Fraud Fusion Taskforce MOU and Taskforce ToR, which should be read in conjunction with this document (the IDC ToR).
- 2.2 The IDC is the governing body for the Fraud Fusion Taskforce. It provides strategic direction and oversight of the effective and efficient operation of the Fraud Fusion Taskforce and its performance against the deliverables. Committee members will represent the interests of their home agency whilst applying a whole-of-government lens. The IDC oversees and guides other Fraud Fusion Taskforce committees and provides advice to participating agencies in pursuit of the Fraud Fusion Taskforce objectives and deliverables (refer to Figure 1 outline of governance structure in Schedule 1).
- 2.3 The IDC will report through agency head to the Minister for the NDIS and Government Services.

3. Membership

3.1 The IDC comprises:

- 3.1.1 Co-Chair and permanent member – NDIA Chief Transformation Officer
- 3.1.2 Co-Chair and permanent member – Services Australia Deputy CEO.
- 3.1.3 Permanent members: Senior Executive Service (SES) officers at Band 2 or above from NDIA, Services Australia, ACIC, ATO, AFP, NQSC and AGD (that are Parties to the Fraud Fusion Taskforce MOU) with expertise or responsibility for delivering taskforce program level strategy or related operational activities, per Table 1 in Schedule 1.
- 3.1.4 Permanent members may agree to include additional Parties to the Fraud Fusion Taskforce MOU as additional permanent or temporary members of the IDC. This may be ongoing membership (permanent member) or for one or more specific agenda items or meetings (temporary member) – refer Table 1 in Schedule 1 where ongoing new members will be identified.
- 3.1.5 For the IDC, proxy representation is allowed, however not below SES Band 2 Level for members (that are not Co-Chairs) except with the approval of both Co-Chairs. The Co-Chairs can be proxy for each other; or if neither is available, they can assign a proxy of their choice.

3.2 Permanent observers to the IDC include the Co-Chairs of the Intelligence Operations Committee (IOC) and the Strategic Prevention Committee (SPC) (unless these IOC and SPC Co-Chairs are already members of the IDC; in which case they would contribute as members). Other observers may be determined by the IDC.

3.3 As required, each IDC Co-Chair may request additional invitees or observers to attend committee meetings. Participating agency staff and external experts may be invited to address issues that require subject matter expertise.

Note: Consideration of meeting attendees will have regard to intelligence and information sharing arrangements including risk in sharing of ACIC and other intelligence.

4. Reporting relationships

4.1 The IDC will oversee other Fraud Fusion Taskforce committees – refer governance diagram in Figure 1 Schedule 1.

4.2 Engagement between the IDC and the other committees will be facilitated by the Fraud Fusion Taskforce Co-Chairs, supported by the Taskforce Management Office (TMO).

5. Functions

5.1 Complementing and meeting the responsibilities outlined in clause 1, the IDC will provide strategic direction and oversight of the Fraud Fusion Taskforce, including:

- 5.1.1 Facilitating compliance of the Parties with the Fraud Fusion Taskforce MOU.
- 5.1.2 Defining the strategic priorities for the Fraud Fusion Taskforce, including strategic intelligence priorities, and referring these to other Fraud Fusion Taskforce committees for action.

Fraud Fusion Taskforce – Inter-Departmental Committee Terms of Reference

- 5.1.3 Overseeing the effective operation of other Fraud Fusion Taskforce committees and working groups as considered appropriate by the IDC.
- 5.1.4 Defining the prioritisation and scope for inclusion in the Fraud Fusion Taskforce of government programs and payments in addition to the NDIS.
- 5.1.5 Overseeing the effective operation of the Fraud Fusion Taskforce, and other inter-agency cooperation, to deliver on the strategic priorities of the Fraud Fusion Taskforce.
- 5.1.6 Reviewing and making decisions on key strategic level deliverables and artefacts of the Fraud Fusion Taskforce, that may be referred from the other Fraud Fusion Taskforce committees.
- 5.1.7 Considering risks escalated from supporting committees and working groups and agreeing mitigation strategies.
- 5.1.8 Ensuring communication protocols are established and effective for the Fraud Fusion Taskforce; these will provide whole-of-government messaging and insights.
- 5.1.9 Exchanging information and strategic insights around serious and organised crime and fraud-related risks and activities impacting on the NDIS and other Australian Government programs and payments, as outlined in the MOU and Fraud Fusion Taskforce ToR.
- 5.1.10 Supporting the development of longer-term scalable fraud prevention, detection and investigation capability across Government.
- 5.1.11 Identifying and agreeing on opportunities for collaborative arrangements between Australian Government agencies to facilitate information exchange and development of fraud intelligence and insights for effective fraud prevention and treatment.
- 5.1.12 Engaging with other related government committees and stakeholders to manage the interconnections between the Fraud Fusion Taskforce, partner agencies, and other Australian Government agencies.
- 5.2 The IDC may appoint one or more working groups to assist with its function where required.
- 5.3 The IDC will provide the CEO of NDIA and CEO of Services Australia with timely, accurate, insightful and accessible advice and recommendations about the Fraud Fusion Taskforce's:
 - 5.3.1 Strategic and governance framework.
 - 5.3.2 Resourcing and funding.
 - 5.3.3 Performance and deliverables.
 - 5.3.4 Communications and insights.

6. Secretariat

- 6.1 Secretariat support for the IDC will be provided by the Fraud Fusion TMO managed by NDIA.

Fraud Fusion Taskforce – Inter-Departmental Committee Terms of Reference

- 6.2 Secretariat services will include managing the agenda, minutes, registers and other administrative arrangements for the IDC.

7. Meeting arrangements

- 7.1 The Co-Chairs will choose which Co-Chair will preside at each committee meeting or nominate an IDC member to preside as Alternate Chair (SES Band 2 level or above).
- 7.2 The committee will meet, approximately six weekly, on dates set by the Co-Chairs in consultation with committee members.
- 7.3 Meetings will be a mix of face-to-face and secure videoconference or teleconference, as agreed by members.
- 7.4 Agenda IDC meetings will be approved by both IDC Co-Chairs and distributed to IDC members no later than five working days before a meeting.
- 7.5 Decisions and actions will be recorded in minutes for all meetings.
- 7.6 Out-of-session matters may be considered by the committee as appropriate to ensure timeliness of IDC business.
- 7.7 Subject to subclause 7.8, motions will be carried by IDC based on either:
- 7.7.1 Unanimous decision of all permanent members attending (including the Chair) for the meeting (preferred); OR
 - 7.7.2 A simple majority of affirmative member votes (each member for that item has 1 vote to cast).
- 7.8 IDC matters for agreement (motions) will not be considered carried, i.e., affirmed by the IDC, if the matter/s concern a program or payment administered by a Party who is not in attendance or chooses not to affirm the decision.
- 7.9 At least three (3) permanent members (exclusive of Co-Chairs) must be in attendance for an IDC meeting to go ahead. NDIA and Services Australia must also be in attendance.
- 7.10 All members are expected to:
- 7.10.1 Act in accordance with APS values.
 - 7.10.2 Bring forward papers which enable the IDC to discharge its responsibilities.
 - 7.10.3 Act in a collegiate and collaborative manner when discussing and resolving issues.
 - 7.10.4 Provide the committee with accurate and timely information to enable well-informed reporting.
 - 7.10.5 Declare and avoid conflicts of interest and conflicts of role.
- Note:** Parties will set up their own governance frameworks to feed in appropriate and timely information to the IDC, including as facilitated by the TMO.

Fraud Fusion Taskforce – Inter-Departmental Committee Terms of Reference

8. Communication and information dissemination protocol

- 8.1 The IDC will have regard to the MOU for the Fraud Fusion Taskforce in respect of information and communication protocols.
- 8.2 IDC minutes will be distributed to members for that meeting, permanent observers, the IOC and the SPC and any other stakeholders approved by a Co-Chair of the IDC.

9. Review of terms of reference

- 9.1 These terms of reference will be reviewed by the IDC at least once every twelve months, or after any significant change in respect of the Fraud Fusion Taskforce scope and mandate or changes in member agencies.
- 9.2 These terms of reference were last reviewed on 22 May 2023.

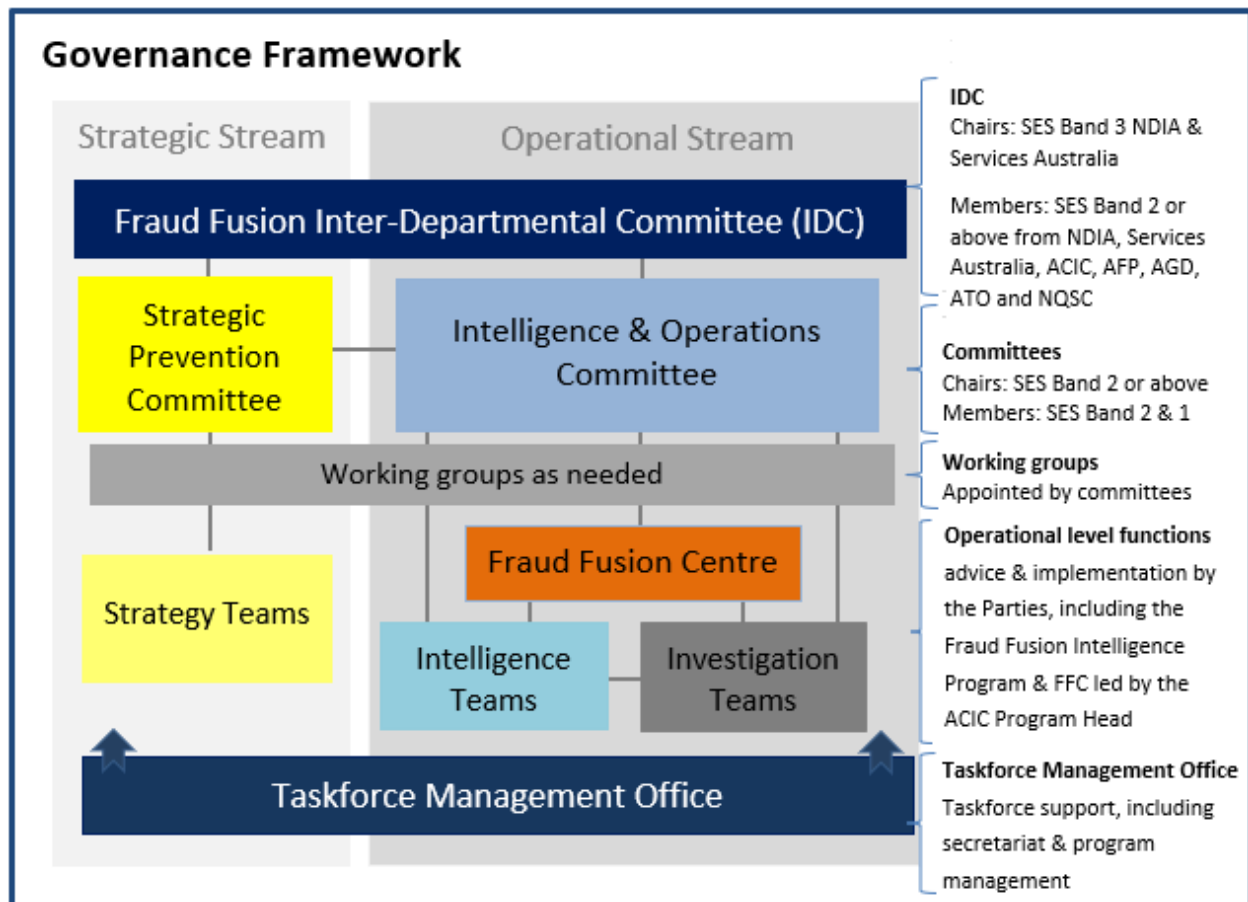
 Fraud Fusion Taskforce – Inter-Departmental Committee Terms of Reference

Schedule 1**Table 1 – IDC Membership**

Organisation	Position Title	Role
National Disability Insurance Agency	Chief Transformation Officer	Co-Chair and Permanent Member
Services Australia	Deputy CEO, Payments and Integrity	Co-Chair and Permanent Member
Australian Criminal Intelligence Commission	Executive Director Intelligence Operations	Permanent Member
Australian Taxation Office	Deputy Commissioner, Fraud & Criminal Behaviours	Permanent Member
Australian Federal Police	Deputy Commissioner Crime	Permanent Member
Attorney-General's Department	First Assistant Secretary, Integrity Frameworks Division	Permanent Member
NDIS Quality and Safeguards Commission	Commissioner	Permanent Member
National Disability Insurance Agency	Director Taskforce Management Office	Secretariat
Temporary Members and Observers will be determined by the IDC / Co-Chairs as outlined in the IDC ToR		

Fraud Fusion Taskforce – Inter-Departmental Committee Terms of Reference

Figure 1 – Fraud Fusion Taskforce Governance Structure





Australian Government
Fraud Fusion Taskforce

Terms of Reference

Intelligence and Operations Committee

Dated: 27 May 2026

Approved Version: V1.0

Table of Contents

1. Background	3
2. Purpose	3
3. Functions	3
4. Sub-Committee and External Advice.....	4
5. Escalation	4
6. Membership	4
7. Confidentiality	5
8. Disclosure of Interests	5
9. Secretariat	5
10. Meeting Arrangements.....	6
11. Communication and Reporting.....	7
12. Review of Terms of Reference.....	7
Schedule 1 – Intelligence and Operations Committee Protocols	9
Schedule 2 – FFT Governance Structure	11

1. Background

- 1.1 Fraud Fusion Taskforce (FFT) has been formed to strengthen the Commonwealth's fraud detection, prevention, and response capability through enhanced data-sharing and intelligence, a coordinated government approach to detection and treatment of serious and organised crime and systemic fraud, and well-informed cross-program actions to help prevent fraud. This will draw on the capabilities and powers of the agencies that are Parties to the Memorandum of Understanding (MOU) for the FFT.
- 1.2 The FFT will develop multi-agency capability, an enhanced government intelligence base and create scalable solutions to prevent, detect and respond to fraud affecting the National Disability Insurance Scheme (NDIS) and other Australian government programs and payments, and Australians who are intended participants and recipients. This will result in reduced 'waste' due to fraud, non-compliance and incorrect payments and impacts for participants and intended stakeholders of such programs.
- 1.3 The FFT governance structure incorporates three committees, including Operational Intelligence Committee (IOC) Schedule 2 which outlines the FFT governance structure.
- 1.4 The FFT Terms of Reference (ToR) (Subclause 3(7)) state that the IOC may establish working groups to assist with its functions. As a sub-committee of the FFT Inter-Departmental Committee (IDC), the IOC can establish working groups to facilitate its operational objectives. These working groups are set out in section 4.
- 1.5 The terms of reference will be agreed by the IOC and IDC and formally recorded in the Committee meeting minutes. Sub-groups will report to the IOC.
- 1.6 Definitions of key terms, expressions and acronyms used in this IOC ToR are the same as defined in the FFT MOU and ToR.

2. Purpose

- 2.1 These ToR establish the mandate, scope and governance arrangements for the FFT Intelligence and Operations Committee (IOC) and describe how members will work collectively to support the objectives of the FFT, in accordance with the FFT MOU and the FFT ToR.
- 2.2 The purpose of the IOC is to provide strategic oversight of intelligence and operational activities undertaken as part of the FFT, to ensure the FFT operational and intelligence objectives are achieved, including agreed savings and integrity outcomes.
- 2.3 The IOC supports whole of FFT coherence by sharing relevant information with, and receiving strategic advice from, the Strategic Prevention Committee (SPC) the Operational Working Group (OWG) and the Data Sharing Working Group (DSWG), where this is necessary to inform IOC decision making.

3. Functions

- 3.1 The IOC performs the following functions in support of FFT objectives:
 - 3.1.1 Provide oversight of FFT intelligence and operational activities to ensure delivery against agreed FFT objectives, priorities, savings and integrity outcomes.
 - 3.1.2 Oversee FFT cases, DSWG data sharing activities, FFT projects and operations, including reviewing new case referrals from the OWG, monitoring progress and performance against objectives.
 - 3.1.3 Manage FFT shared operational and intelligence risks in accordance with IDC approved risk settings, including overseeing relevant risk and ethics registers, supporting ethical decision-making, documenting and escalating risk and ethical matters and reporting to IDC (and SPC where appropriate).
 - 3.1.4 Identify, promote and progress opportunities for cross-agency collaboration,

intelligence and data sharing, and coordinated treatments across prevention, investigation and enforcement responses, including leveraging specialist capabilities and support from FFT agencies, committees and external partners where appropriate.

- 3.1.5 Consider agency capacity and capability to deliver against joint areas of risk or operational interest, identify constraints or gaps and escalate issues or recommendations to IDC where required.
- 3.1.6 Ensure IOC activities, decisions and prioritisation are aligned with FFT, IDC, SPC, OWG and DSWG working programs and priorities, and share operational feedback and insights to support coherent whole of FFT delivery.
- 3.1.7 Consider the potential role of external tools/stakeholders to support the identification, assessment and treatment of fraud risks.
- 3.1.8 Support IDC as required within the IOC's remit.

4. Sub-Committee and External Advice

- 4.1 The IOC may commission or engage with subcommittees, working groups or external advisory bodies where required, including but not limited to:
 - 4.1.1 Strategic Prevention Committee (SPC)
 - 4.1.2 OWG
 - 4.1.3 DSWG
 - 4.1.4 Joint Analyst Group (JAG)
 - 4.1.5 Other expert FFT forums and advisory mechanisms approved by the Co-Chairs.

5. Escalation

- 5.1 The Co-Chairs may, with their discretion, escalate any opportunities to the IDC.
- 5.2 The Co-Chairs must escalate where:
 - 5.2.1 Agreement cannot be reached in accordance with these ToR.
 - 5.2.2 A risk or ethical issue has been identified and requires oversight and mitigation by IDC. For example, new risks or increased risk ratings for existing risks or an ethical issue requires escalation.
 - 5.2.3 Ethical issues have been identified. Members may raise ethical matters confidentially with the IDC Co-Chairs and/or Chairs/Co-Chairs of committees and working groups.

6. Membership

- 6.1 The IOC comprises of:
 - 6.1.1 Co-Chair and permanent member – National Disability Insurance Agency (NDIA), SES Band 2 (who may also be an observer or member of the IDC).
 - 6.1.2 Co-Chair and permanent member – Services Australia, SES Band 2 (who may also be an observer or member of the IDC).
 - 6.1.3 Permanent members at SES Band 1 from agencies specifically funded to participate in the FFT, including the National Disability Insurance Agency (NDIA), Services Australia, Australian Criminal Intelligence Commission (ACIC), Aged Care Quality and Safety Commission (ACQSC), Australian Federal Police (AFP), the Australian Taxation Office (ATO), Department of Health, Disability and Ageing (DHDA), Department of Education (DoE), Department of Veterans Affairs (DVA)

and the NDIS Quality and Safeguards Commission (NQSC).

- 6.1.4 Representatives from other FFT member agencies by request.
- 6.1.5 Representatives from non-member agencies by request.
- 6.1.6 Further permanent or temporary members at the discretion of the IOC Co-Chairs.
- 6.2 Requests to attend an IOC meeting and the reason for attendance should be submitted to the Taskforce Management Office (TMO). Approval will be sought from the Co-Chairs on specific requests to add or replace members, or grant observer status to persons, in accordance with the IOC purposes if there is a relevant need to know/attend. Where approval is granted by the Co-Chairs, the TMO will facilitate attendance by providing the agenda and meeting details to the requestor.
- 6.3 Nominated observers must be at Executive Level 2 or above or at the discretion of Co-Chairs.
- 6.4 Attendees must have minimum 'Negative Vetting 1' security clearance to attend meetings.
- 6.5 Permanent membership of the IOC will be approved by the Co-Chairs with a majority of support from existing IOC members.

7. Confidentiality

- 7.1 Meeting members undertake as follows:
 - 7.1.1 to use any confidential information or personal information provided to them as members of the meeting for the sole purpose of their involvement in the committee; and
 - 7.1.2 not to disclose or reproduce any such confidential Information or personal information to any person without the prior written approval of the Co-Chairs; and
 - 7.1.3 to take all necessary precautions to prevent unauthorised access to or copying of any such confidential information and personal information in the meeting member's control.

8. Disclosure of Interests

- 8.1 A meeting member who has an interest, pecuniary or otherwise, in a matter being considered, or about to be considered by the meeting, must disclose the nature of the interest to the Co-Chairs.
- 8.2 The disclosure must be made as soon as possible after the relevant facts have come to the meeting members' knowledge.
- 8.3 The Co-Chairs may decide that the member making the disclosure does not participate in decision-making regarding the matter, or that the member does not attend the meeting discussion in relation to that matter.
- 8.4 The disclosure, and the action taken in relation to it, must be recorded in the minutes of the meeting.

9. Secretariat

- 9.1 Secretariat services for the IOC will be provided by the TMO.
- 9.2 Secretariat services will include managing:
 - 9.2.1 Preparation and distribution of meeting agendas and papers.
 - 9.2.2 Recording of minutes and tracking of actions.
 - 9.2.3 Recording of identified risks, ethical issues, and conflicts of interest raised at meetings, and supporting escalation processes where required.

- 9.2.4 Out of session considerations and endorsements.
- 9.2.5 Coordination of engagement between the IOC and other committees and working groups, as required; and
- 9.2.6 Membership records, including changes to membership and membership requests.
- 9.3 Non-members may provide input or feedback to committees and working groups through engagement with the TMO.
- 9.4 Full records of working group meetings, including agenda, submission papers, minutes, and out of session submissions fall under the responsibility of TMO Secretariat.

10. Meeting Arrangements

Meeting agenda, papers and minutes

- 10.1 The agenda and papers are to be approved by Co-Chairs in advance of the meeting date and where possible, provided to meeting members 3 business days prior to a meeting.
- 10.2 The duration of meetings is limited to one and half hours.
- 10.3 The standing items for each meeting are:
 - 10.3.1 Welcome, apologies and actions items
 - 10.3.2 Operational Working Group updates
 - 10.3.3 ACIC Fraud Fusion Centre (FFC) Update
 - 10.3.4 Risk and Ethics considerations
 - 10.3.5 Other business
 - 10.3.6 Action items and close
- 10.4 Decisions and actions will be recorded in minutes for all meetings. Decisions and action registers will be maintained by the Secretariat.
- 10.5 Parties will set up their own governance frameworks to feed appropriate and timely information to the IOC.
- 10.6 Agreed actions will be updated by the Secretariat and form the primary minutes for meetings.

Quorum Requirements

- 10.7 For a meeting to be recognised as an authorised meeting and recommendations or resolutions to be valid, a minimum of three IOC permanent member agencies (Refer to membership 6.1.3) must be in attendance.
- 10.8 The required quorum for endorsement of out-of-session cases will be:
 - 10.8.1 Three members, which must include Co-Chairs.

Out of session endorsements

- 10.9 Matters can be considered or dealt with out-of-session by the IOC Co-Chairs if deemed appropriate, including timely or urgent actions and decisions.
- 10.10 The IOC may make decisions out-of-session in the following circumstances:
 - 10.10.1 IOC members have been informed of the proposed decision, and,
 - 10.10.2 IOC member agencies entitled to vote on the proposed decision indicate agreement (refer to quorum requirements 10.8.1).
 - 10.10.3 Three members have been informed of the proposed decision, and,

- 10.10.4 Three member agencies entitled to vote on the proposed decision indicate agreement
- 10.11 IOC members indicate agreement to a decision by providing written advice to the meeting secretariat of their agreement.
- 10.12 Out of session decisions must be included for discussion at the next IOC meeting.

Frequency and location

- 10.13 The IOC will meet virtually every 6-7 weeks, on dates set by the Co-Chairs in consultation with members.
- 10.14 Additional meetings can be arranged by the Co-Chairs in relation to other matters or if there are special circumstances.
- 10.15 Joint sittings with the SPC may be held on matters that are of relevance to both the IOC and SPC.
- 10.16 The IOC Co-Chairs will alternate chairing responsibilities.

Conduct of members

- 10.17 All members are expected to:
 - 10.17.1 Ensure all duties are performed in accordance with the APS Code of Conduct and Values.
 - 10.17.2 Provide input into proceedings and drive the IOC to work within and across agencies in a collegiate and collaborative manner.
 - 10.17.3 Provide the IOC with accurate and timely information to enable well-informed reporting on operations and intelligence.
 - 10.17.4 Role modelling ethical behaviour, identifying and escalating ethical matters through the function of committees and working groups, or when undertaking any other FFT activities. Consideration must be given to the values and principles outlined in the guide 'Behaving Ethically: a guide for Taskforce members.
- 10.18 Bring forward papers which enable the IOC to discharge its responsibilities.
- 10.19 Declare and avoid conflicts of interest and conflicts of role.

Proxies to Meetings

- 10.20 Members of the IOC can nominate a proxy to attend a meeting if the member is unable to attend (refer to membership 6.2).
- 10.21 Approval must be sought from the Co-Chair prior to the scheduled nominated meeting.

11. Communication and Reporting

- 11.1 IOC minutes may be shared with IDC, and SPC where appropriate (with regard to risk management and legislative considerations) by the TMO on endorsement of Chair.
- 11.2 The minutes, or an extract or summary thereof, may be distributed to other agencies or stakeholders who are not Parties in relation to specific needs agreed at IOC (with appropriate regard to risk and legislative considerations).

12. Review of Terms of Reference

- 12.1 The IOC ToR:
 - 12.1.1 are subject to IDC endorsement, and;

12.1.2 will be reviewed by the IOC at least once every twelve months or after any significant change in respect of the FFT scope and mandate.

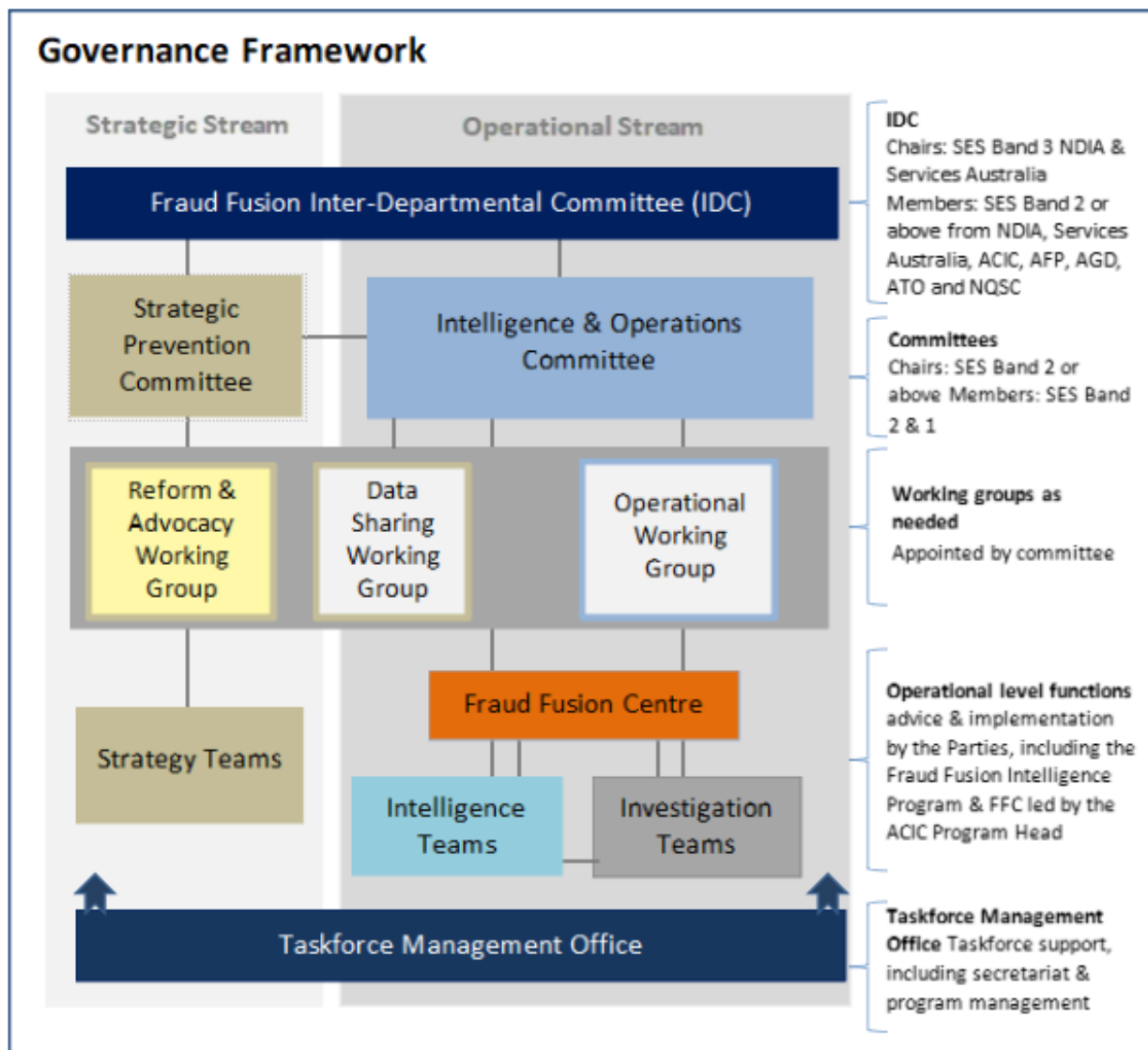
12.2 This ToR was last reviewed on 27 May 2026.

Schedule 1 – Intelligence and Operations Committee Protocols

Roles	Responsibilities	Requirements
Co-Chairs	The Co-Chairs are to ensure meetings are held in accordance with the working group's ToR and are run effectively and inclusively. The Co-Chairs have the authority to not accept a submission if the paper is inappropriately scoped, containing inaccurate or unsubstantiated information or information which has not been cleared through the appropriate channels. The Co-Chairs are to facilitate and contribute to the functional and operational reviews and approve the role and relevance of the working group. The Co-Chairs have the authority to delegate any of the above tasks to a nominated member or representative.	☐ SES Band 2 ☐ Negative Vetting 1 Security Clearance
Members	Members are to ensure the working group's purpose is met by effectively contributing to the working group's business. The role of members is to contribute to the effective operations of the meeting and progress all matters requested by the working group.	☐ SES Band 1 ☐ Negative Vetting 1 Security Clearance ☐ Co-Chair approval required for new members
Proxy	A proxy acts on behalf of a member who cannot attend the meeting for a period of time. This person is usually designated to represent the absent members' interest and must be endorsed by a Co-Chair to attend.	☐ SES Band 1 or Min EL2 or at discretion of Co-Chairs ☐ Co-Chair Endorsement ☐ Negative Vetting 1 Security Clearance ☐ Reason/term for proxy request
Observers	Observers do not contribute to the meeting or to decision making in any way. They are to act in accordance with the Co-Chairs requests. Temporary observers may be granted access to a meeting and must be endorsed by a Co-Chair to attend.	☐ Min. EL2 or at the discretion of Co-Chairs ☐ Co-Chair Endorsement ☐ Negative Vetting 1 Security Clearance ☐ Permanent or temporary arrangement
Guests	The role of a Guest is to provide information on specific topics. Guests may be granted access to a meeting and must be endorsed by the Chair to attend. Guests only attend for their item and do not make decisions.	☐ Co-Chair Endorsement ☐ Min. EL1 or at the discretion of Co-Chairs ☐ Negative Vetting 1 Security Clearance ☐ Reason for attendance (e.g. agenda item/full meeting)

Secretariat	The Secretariat supports the Chair and members to ensure the working group meetings are managed effectively and in accordance with the committee's ToR. The Secretariat is to manage proceedings as specified by the Co-Chairs.	☐ Co-Chair Endorsement ☐ Negative Vetting 1 Security Clearance
--------------------	---	---

Schedule 2 – FFT Governance Structure





Australian Government
Fraud Fusion Taskforce

Terms of Reference

Strategic Prevention Committee

Dated: 27 May 2026

Approved Version: V1.0

Table of Contents

1. Background.....	3
2. Purpose	3
3. Functions	3
4. Sub-Committee and External Advice.....	4
5. Escalation	4
6. Membership	4
7. Confidentiality	5
8. Disclosure of Interests	5
9. Secretariat	5
10. Meeting Arrangements.....	6
11. Communication and Reporting.....	7
12. Review of Terms of Reference.....	7
Schedule 1 – Strategic Prevention Committee Protocols	9
Schedule 2 – Fraud Fusion Taskforce Governance Structure.....	11

1. Background

- 1.1 Fraud Fusion Taskforce (FFT) has been formed to strengthen the Commonwealth's fraud detection, prevention, and response capability through enhanced data-sharing and intelligence, a coordinated government approach to detection and treatment of serious and organised crime and systemic fraud, and well-informed cross-program actions to help prevent fraud. This will draw on the capabilities and powers of the agencies that are Parties to the Memorandum of Understanding (MOU) for the FFT.
- 1.2 The FFT will develop multi-agency capability, an enhanced government intelligence base and create scalable solutions to prevent, detect and respond to fraud affecting the National Disability Insurance Scheme (NDIS) and other Australian government programs and payments, and Australians who are intended participants and recipients. This will result in reduced 'waste' due to fraud, non-compliance and incorrect payments and impacts for participants and intended stakeholders of such programs.
- 1.3 The FFT governance structure incorporates three committees, including the Strategic Prevention Committee (SPC). Schedule 2, which outlines the FFT governance structure.
 - 1.3.1 Fraud Fusion Centre Advisory Group (FFCAG) has been removed from the FFT governance structure as this does not have formal TMO governance oversight and is led by Australian Criminal Intelligence Commission (ACIC) when required.
- 1.4 The FFT Terms of Reference (ToR) (Subclause 3(7)) state that the SPC may establish working groups to assist with its functions. These working groups are set out in section 4.
- 1.5 Definitions of key terms, expressions and acronyms used in this SPC ToR are the same as defined in the FFT MOU and ToR.

2. Purpose

- 2.1 These ToR establish the mandate, scope and governance arrangements for the FFT SPC and describe how members will work collectively to support the objectives of the FFT, in accordance with the FFT MOU and FFT ToR.
- 2.2 The purpose of the SPC is to oversee and direct the forward-looking strategic prevention strategy for FFT activities and ensure the longer-term fraud prevention purpose of the FFT is met.
- 2.3 The SPC will share information with the Intelligence and Operations Committee (IOC) when this is required to provide advice on the intelligence and operational strategy. The SPC will receive operational and intelligence advice from the IOC and Fraud Fusion Centre to inform decisions.

3. Functions

- 3.1 The SPC performs the following functions in support of FFT objectives:
 - 3.1.1 Oversee the development, testing evaluation and implementation of innovative and scalable fraud prevention controls, assurance approaches and maturity models to facilitate provision of strategic advice and recommendations to the IDC and IOC.
 - 3.1.2 Identify, assess and respond to forward-looking strategic risks and government payment integrity vulnerabilities within FFT remit.
 - 3.1.3 Facilitate and manage ethics related discussions, support ethical decision making, document ethical matters and ensure appropriate escalation of ethical issues in accordance with FFT governance arrangements.
 - 3.1.4 Identify, leverage and progress opportunities for cross-agency collaboration, including strategic prevention initiatives, data sharing, and application of treatments, while considering agency capacity and capability to deliver against

join areas of risk or interest.

- 3.1.5 Ensure SPC activities and prioritisation are aligned with FFT, IDC, IOC, RAWG and other relevant committee functions, work programs and priorities, and provide strategic feedback and insights to support coordinated delivery of FFT objectives.
- 3.1.6 Focus on strategies that protect the identities and safety of participants and genuine providers from fraud, particularly serious and organised crime entities, and address risks that impact participant safety and service quality.
- 3.1.7 Consider the potential for external tools/stakeholders including professional associations, care economy and communities of practice, to support the identification and/or treatment of risks within the remit of the FFT.
- 3.1.8 Support IDC as required within the SPC's remit.

4. Sub-Committee and External Advice

- 4.1 The SPC may commission or engage with sub-committees, working groups or external advisory bodies where required, including but not limited to:
 - 4.1.1 Financial Crime and Money Laundering (FCML) working groups
 - 4.1.2 Data Sharing Working Group (DSWG)
 - 4.1.3 Reform Advocacy Working Group (RAWG)
 - 4.1.4 International Public Sector Fraud Forum (IPSFF)
 - 4.1.5 Communities of Practice; and
 - 4.1.6 Other expert advisory mechanisms approved by the Chair

5. Escalation

- 5.1 The Co-Chairs may, at their discretion, escalate any opportunities to the IDC.
- 5.2 The Co-Chairs **must** escalate where:
 - 5.2.1 Agreement cannot be reached in accordance with these ToR.
 - 5.2.2 A risk or ethical issue has been identified and requires oversight and mitigation by IDC. For example, new risks or increased risk ratings for existing risks, or an ethical issue requires escalation.
 - 5.2.3 Ethical issues have been identified. Members may raise ethical matters confidentially with the IDC Co-Chairs and/or Chairs/Co-Chairs of committees and working groups.

6. Membership

- 6.1 The SPC comprises of:
 - 6.1.1 Co-Chair and permanent member – National Disability Insurance Agency (NDIA), SES Band 2 (who may also be an observer or member of the Inter-Departmental Committee (IDC).
 - 6.1.2 Co-Chair and permanent member – Australian Taxation Office (ATO), SES Band 2 (who may also be an observer or member of the IDC).
 - 6.1.3 Permanent members at SES Band 1 from agencies specifically funded to participate in the FFT, including the National Disability Insurance Agency (NDIA), Services Australia, Australian Criminal Intelligence Commission (ACIC), Australian Federal Police (AFP), Attorney Generals Department (AGD), Australian Taxation Office (ATO), Department of Education (DoE), Department of Veterans Affairs (DVA), NDIS Quality and Safeguards Commission (NDIS Commission), Services

Australia.

- 6.1.4 Representatives from other FFT member agencies by request.
- 6.1.5 Representatives from non-member agencies by request.
- 6.1.6 Further permanent or temporary members at the discretion of the SPC Co-Chairs.
- 6.2 Requests to attend an SPC meeting and the reason for attendance should be submitted to the Taskforce Management Office (TMO). Approval will be sought from the Co-Chairs on specific requests to add or replace members, or grant observer status to persons, in accordance with the SPC purposes if there is a relevant need to know/attend. Where approval is granted by the Co-Chairs, the TMO will facilitate attendance by providing the agenda and meeting details to the requestor.
- 6.3 Nominated observers must be at Executive Level 2 or above or at the discretion of the Co-Chairs.
- 6.4 Attendees must have minimum 'Negative Vetting 1' security clearance to attend meetings.
- 6.5 Permanent membership of the SPC will be approved by the Co-Chairs with a majority of support from existing SPC members.

7. Confidentiality

- 7.1 Meeting members undertake as follows:
 - 7.1.1 To use any confidential information or personal information provided to them as members of the meeting for the sole purpose of their involvement in the committee; and
 - 7.1.2 Not to disclose or reproduce any such confidential information or personal information to any person without the prior written approval of the Co-Chairs; and
 - 7.1.3 To take all necessary precautions to prevent unauthorised access to or copying of any such confidential information and personal information in the meeting member's control.

8. Disclosure of Interests

- 8.1 A meeting member who has an interest, pecuniary or otherwise, in a matter being considered, or about to be considered by the meeting, must disclose the nature of the interest to the Co-Chairs.
- 8.2 The disclosure must be made as soon as possible after the relevant facts have come to the meeting members' knowledge.
- 8.3 The meeting may decide that the member making the disclosure does not participate in decision-making regarding the matter, or that the member does not attend the meeting discussion in relation to that matter.
- 8.4 The disclosure, and the action taken in relation to it, must be recorded in the minutes of the meeting.

9. Secretariat

- 9.1 Secretariat services for the SPC will be provided by the TMO.
- 9.2 Secretariat services will include managing:
 - 9.2.1 The preparation and distribution of meeting agendas and papers.
 - 9.2.2 The recording of minutes and tracking of actions.
 - 9.2.3 The recording of identified risks, ethical issues, and conflicts of interest raised at

meetings, and supporting escalation processes where required.

- 9.2.4 Out of session considerations and endorsements.
- 9.2.5 Coordination of engagement between the SPC and other committees and working groups, as required; and
- 9.2.6 Membership records, including changes to membership and membership requests.
- 9.3 Non-members may provide input or feedback to committees and working groups through engagement with the TMO.
- 9.4 Full records of working group meetings, including agenda, submission papers, minutes, and out of session submissions fall under the responsibility of TMO Secretariat.

10. Meeting Arrangements

Meeting agenda, papers and minutes

- 10.1 The agenda and papers are to be approved by Co-Chairs in advance of the meeting date and where possible, provided to meeting members 3 business days prior to a meeting.
- 10.2 The duration of meetings is limited to one and half hours.
- 10.3 The standing items for each meeting are:
 - 10.3.1 Welcome, apologies and actions items
 - 10.3.2 FFT 2.0 Update
 - 10.3.3 ACIC Fraud Fusion Centre (FFC) Update
 - 10.3.4 Strategic Prevention Update
 - 10.3.5 Risk and Ethics considerations
 - 10.3.6 Other business
 - 10.3.7 Action items and close
- 10.4 Decisions and actions will be recorded in minutes for all meetings. Decisions and action registers will be maintained by the Secretariat.
- 10.5 Parties will set up their own governance frameworks to feed appropriate and timely information to the SPC.
- 10.6 Agreed actions will be updated by the Secretariat and form the primary minutes for meetings.

Quorum Requirements

- 10.7 For a meeting to be recognised as an authorised meeting and recommendations or resolutions to be valid, a minimum of three SPC permanent member agencies (*Refer to membership 6.1.3*) must be in attendance.
- 10.8 The required quorum for endorsement of out-of-session cases will be:
 - 10.8.1 Three members, which must include Co-Chairs.

Out of session endorsements

- 10.9 Matters can be considered or dealt with out-of-session by the SPC Co-Chairs if deemed appropriate, including timely or urgent actions and decisions.
- 10.10 The SPC may make decisions out-of-session in the following circumstances:
 - 10.10.1 SPC members have been informed of the proposed decision, and,
 - 10.10.2 SPC member agencies entitled to vote on the proposed decision indicate

agreement (refer to quorum requirements 10.8.1).

10.10.3 Three members have been informed of the proposed decision, and,

10.10.4 Three member agencies entitled to vote on the proposed decision indicate agreement.

10.11 SPC members indicate agreement to a decision by providing written advice to the meeting secretariat of their agreement.

10.12 Out of session decisions must be included for discussion at the next SPC meeting.

Frequency and location

10.13 The SPC will meet virtually every 6-7 weeks, on dates set by the Co-Chairs in consultation with members.

10.14 Additional meetings can be arranged by the Co-Chairs in relation to other matters or if there are special circumstances.

10.15 Joint sittings with the IOC may be held on matters that are of relevance to both the SPC and IOC.

10.16 The SPC Co-Chairs will alternate chairing responsibilities.

Conduct of members

10.17 All members are expected to:

10.17.1 Ensure all duties are performed in accordance with the APS Code of Conduct and Values.

10.17.2 Provide input into proceedings and drive the SPC to work within and across agencies in a collegiate and collaborative manner.

10.17.3 Provide the SPC with accurate and timely information to enable well-informed reporting on operations and intelligence.

10.17.4 Role modelling ethical behaviour, identifying and escalating ethical matters through the function of committees and working groups, or when undertaking any other FFT activities. Consideration must be given to the values and principles outlined in the guide 'Behaving Ethically: a guide for Taskforce members.

10.18 Bring forward papers which enable the SPC to discharge its responsibilities.

10.19 Declare and avoid conflicts of interest and conflicts of role.

Proxies to Meetings

10.20 Members of the SPC can nominate a proxy to attend a meeting if the member is unable to attend (*refer to membership 6.2*).

10.21 Approval must be sought from the Co-Chair prior to the scheduled nominated meeting.

11. Communication and Reporting

11.1 SPC minutes may be shared with IDC and IOC where appropriate (with regard to shared information risk and legislative considerations) by the TMO on endorsement of Chair.

11.2 The minutes, or an extract or summary thereof, may be distributed to other agencies or stakeholders who are not Parties in relation to specific needs agreed at SPC (with appropriate regard to risk and legislative considerations).

12. Review of Terms of Reference

12.1 The SPC ToR:

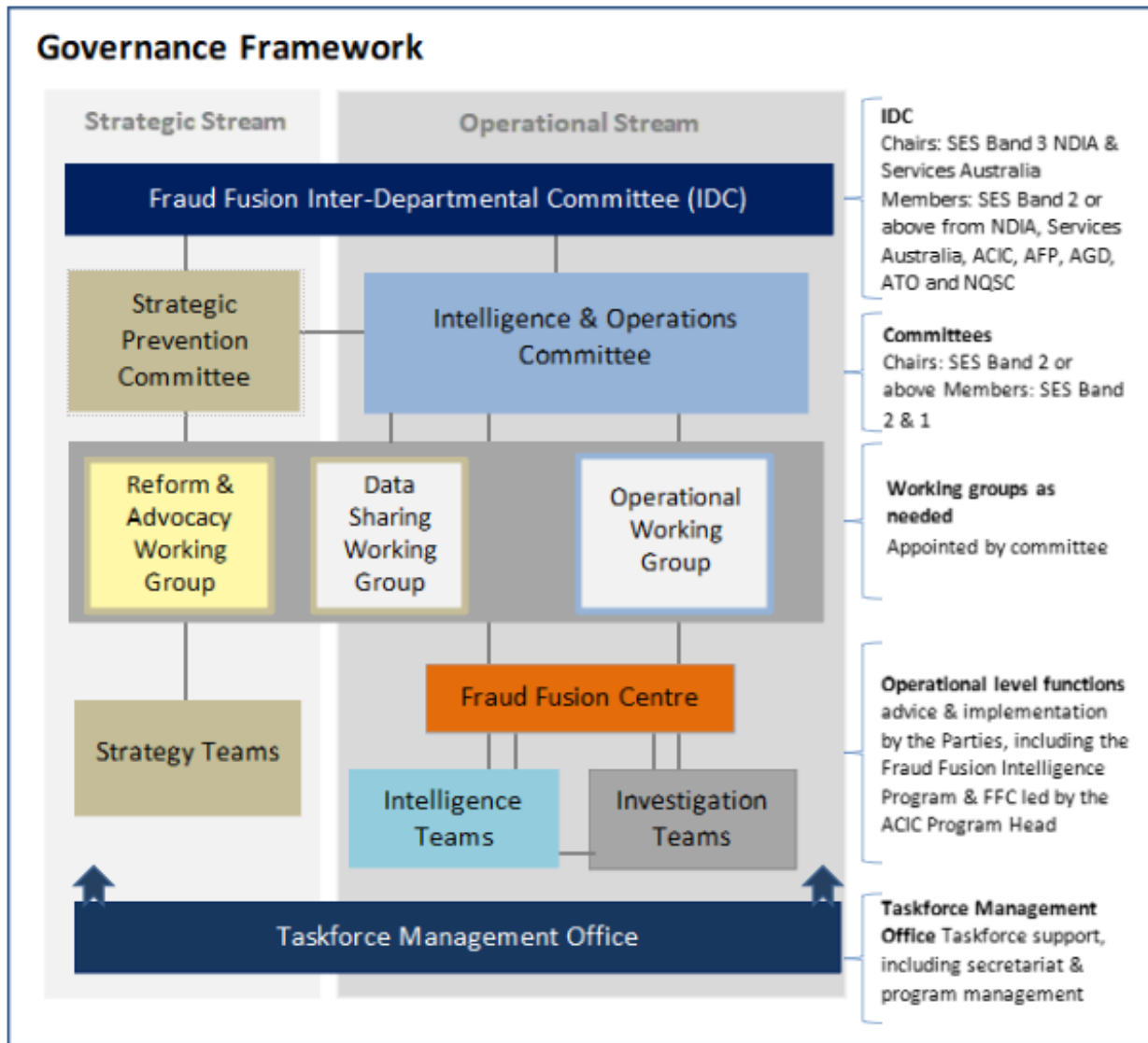
- 12.1.1 are subject to IDC endorsement, and;
 - 12.1.2 will be reviewed by the SPC at least once every twelve months or after any significant change in respect of the FFT scope and mandate.
- 12.2 This ToR was last reviewed on 27 May 2026.

Schedule 1 – Strategic Prevention Committee Protocols

Roles	Responsibilities	Requirements
Co-Chairs	The Co-Chairs are to ensure meetings are held in accordance with the working group's ToR and are run effectively and inclusively. The Co-Chairs have the authority to not accept a submission if the paper is inappropriately scoped, containing inaccurate or unsubstantiated information or information which has not been cleared through the appropriate channels. The Co-Chairs are to facilitate and contribute to the functional and operational reviews and approve the role and relevance of the working group. The Co-Chairs have the authority to delegate any of the above tasks to a nominated member or representative.	☐ SES Band 2 ☐ Negative Vetting 1 Security Clearance
Members	Members are to ensure the working group's purpose is met by effectively contributing to the working group's business. The role of members is to contribute to the effective operations of the meeting and progress all matters requested by the working group.	☐ SES Band 1 ☐ Negative Vetting 1 Security Clearance ☐ Co-Chair approval required for new members
Proxy	A proxy acts on behalf of a member who cannot attend the meeting for a period of time. This person is usually designated to represent the absent members' interest and must be endorsed by a Co-Chair to attend.	☐ SES Band 1 or Min EL2 or at discretion of Co-Chairs ☐ Co-Chair Endorsement ☐ Negative Vetting 1 Security Clearance ☐ Reason/term for proxy request
Observers	Observers do not contribute to the meeting or to decision making in any way. They are to act in accordance with the Co-Chairs requests. Temporary observers may be granted access to a meeting and must be endorsed by a Co-Chair to attend.	☐ Min. EL2 or at the discretion of Co-Chairs ☐ Co-Chair Endorsement ☐ Negative Vetting 1 Security Clearance ☐ Permanent or temporary arrangement
Guests	The role of a Guest is to provide information on specific topics. Guests may be granted access to a meeting and must be endorsed by the Chair to attend. Guests only attend for their item and do not make decisions.	☐ Co-Chair Endorsement ☐ Min. EL1 or at the discretion of Co-Chairs ☐ Negative Vetting 1 Security Clearance ☐ Reason for attendance (e.g. agenda item/full meeting)

Secretariat	The Secretariat supports the Chair and members to ensure the working group meetings are managed effectively and in accordance with the committee's ToR. The Secretariat is to manage proceedings as specified by the Co-Chairs.	☐ Co-Chair Endorsement ☐ Negative Vetting 1 Security Clearance
--------------------	---	--

Schedule 2 – Fraud Fusion Taskforce Governance Structure



OFFICIAL



Australian Government
Fraud Fusion Taskforce

Risk Management Strategy 2024

Version: V0.8
Date: August 2024
Author: NDIA Fraud Fusion Taskforce and Integrity Capability Division
Commencement: Endorsed by IDC on 6 August 2024.

OFFICIAL

Contents

Risk Management Strategy 2024 1

Contents 2

1. Introduction 3

1.1 Legislation and Resources 3

1.2 Consultation 3

1.3 Contact Officer 3

2. FFT Approach to Risk Management 4

2.1 Purpose 4

2.2 Context and environment 4

2.3 FFT Risk Management Framework 4

2.4 FFT Governance Structure 5

2.5 Embedding risk management 6

2.6 Roles and Responsibilities 7

3. Positive Risk Culture 9

4. Risk Appetite and Tolerance 9

4.1 Variations in Risk Rating and Tolerance 10

5. Risk Management Process 10

5.1 FFT Risk classification 10

5.2 FFT Shared Risk 10

5.3 Management of FFT Shared Risk 12

5.4 FFT Risk Management Process 13

6. Managing the Framework 15

6.1 Reporting 15

6.2 Post implementation Review 17

OFFICIAL

1. Introduction

The Fraud Fusion Taskforce (FFT) is committed to establishing an effective system of risk oversight and management, to appropriately manage shared material risks in relation to the FFT's activities in achieving its purpose and objectives.

The FFT Risk Management Strategy (the Strategy) outlines the risk management framework for the FFT and includes:

- a summary of the FFT's approach to risk management
- a summary of the key roles and responsibilities in managing risk
- FFT's risk appetite and tolerance
- the FFT's risk culture
- the management of shared risks and
- the risk management process.

1.1 Legislation and Resources

The FFT Risk Management Strategy has been prepared to align with best practice as follows:

- *Public Governance, Performance and Accountability Act 2013*
- *Public Governance, Performance and Accountability Rule (PGPA Rule) 2014*
- Commonwealth Risk Management Policy
- AS/NZS ISO 31000 Risk Management.

1.2 Consultation

The FFT Risk Management Strategy has been developed in consultation with the Parties of the MOU (20 member agencies), FFT Inter-Departmental Committee (IDC), FFT Committees, and the Taskforce Management Office (TMO).

1.3 Contact Officer

Any queries about the FFT Risk Management Strategy should be directed to
s 47E(d) @ndis.gov.au.

OFFICIAL

2. FFT Approach to Risk Management

2.1 Purpose

The Strategy outlines the FFT's approach to embedding risk management into the governance, decision-making and operations of the FFT. This ensures appropriate oversight of shared material risks is maintained in relation to the FFT's activities in achieving its purpose and objectives.

2.2 Context and environment

The Commonwealth is committed to the safety and wellbeing of all NDIS participants and Australian recipients of government payments and programs and supports and making sure NDIS funding and other government funding is used appropriately.

The FFT was established in November 2022. It is a multi-agency partnership co-led by NDIA and Services Australia, with 20 other government agencies including the NDIS Quality and Safeguards Commission (NDIS Commission), Australian Taxation Office (ATO), Australian Federal Police (AFP) and the Australian Criminal Intelligence Commission (ACIC).

The purpose of the Fraud Fusion Taskforce is to improve payment integrity in government payments and programs by preventing or reducing fraud and criminal activity within and against government programs (including Serious and Organised Crime (SOC) and systemic fraud), to:

- protect the safety and wellbeing of participants who are at risk of harm as a result of fraud, and related service quality.
- protect public finances and prevent or reduce financial losses.
- ensure appropriate use of funds and the sustainability of the programs.
- improve community confidence in the administration of those payments and programs.

NDIS participants and Australian recipients of GPP are at the heart of everything the FFT does to combat fraud and serious organised crime. Safety and wellbeing of these stakeholders is the highest priority. The FFT will have primary regard to risks arising for participants and recipients when considering relevant and appropriate treatment options in relation to fraud and integrity matters.

2.3 FFT Risk Management Framework

OFFICIAL

The FFT is committed to establishing an effective system of oversight to identify, manage, and escalate material shared risks in relation to the FFT's activities in achieving its purpose and objectives.

The FFT Risk Management Framework outlines the FFT's approach to support effective risk management across FFT activity. The FFT Risk Management Strategy and FFT Strategic Risk Register supports the implementation of the FFT Risk Management Framework.

The Strategic Risk Register includes material shared strategic risks to ensure the FFT IDC, and other FFT Committees and working groups, maintain appropriate oversight to support ethical, risk balanced decision-making in relation to the FFT's activity.

2.4 FFT Governance Structure

The governing body of the FFT is IDC co-chaired by NDIA and Services Australia. The IDC has primary responsibility for maintaining appropriate oversight of material shared strategic risks across FFT activities to support risk balanced decision-making.

IDC will be informed by advice and recommendations for strategic and operational risk management made by the FFT Committees; the Strategic Prevention Committee (SPC) and the Intelligence & Operations Committee (IOC) and working groups.

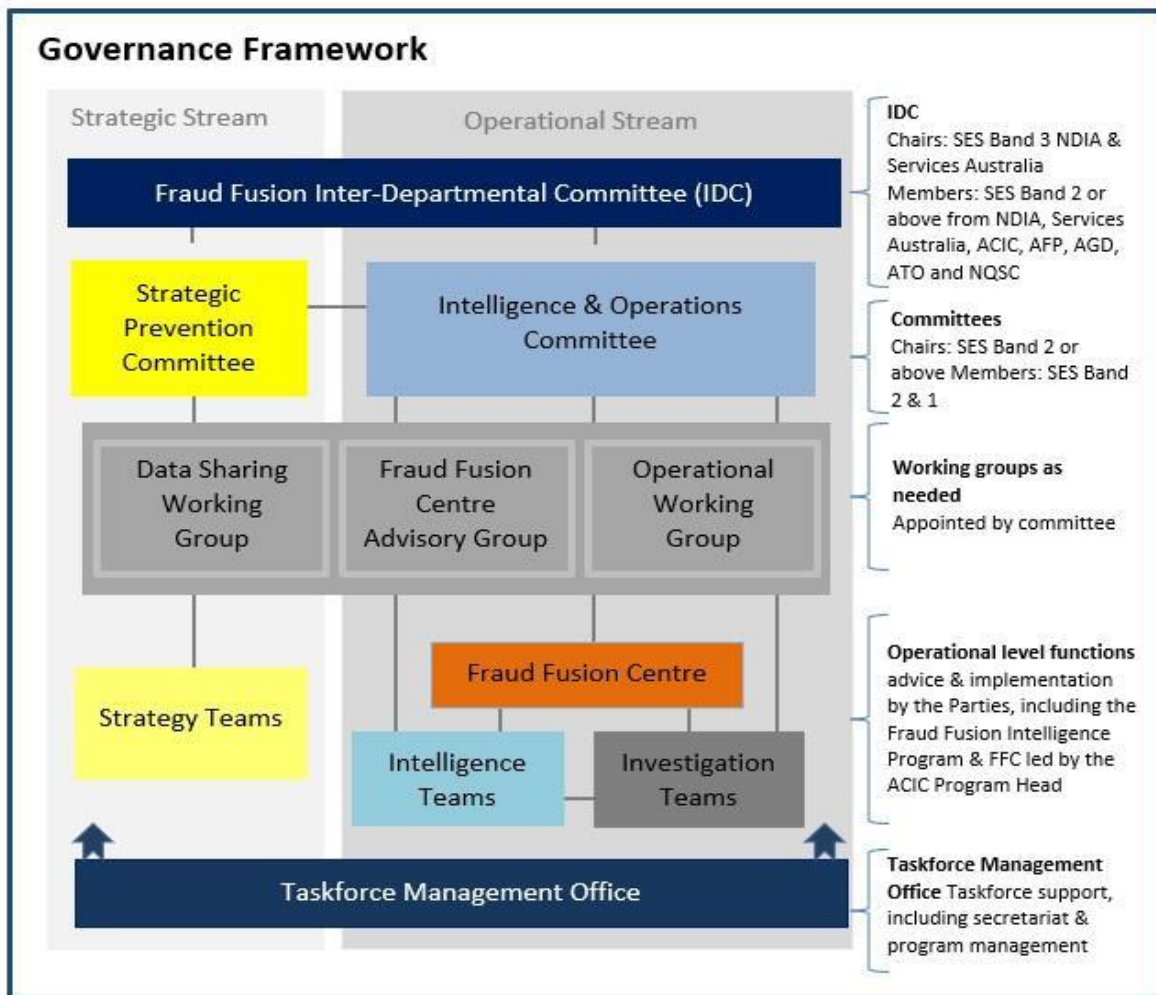
2.4.1 Operational Level Functions

The Australian Criminal Intelligence Commission (ACIC) independently manages the Fraud Fusion Centre (FFC), a centralised mechanism to enable data acquisition, detection analytics and the identification of opportunities for information-sharing for the FFT. The FFC has its own risk management plan and process.

The FFT working groups (Data Sharing Working Group, Operational Working Group and the Fraud Centre Advisory Group managed by the ACIC), have responsibility for advising FFT Committees on implementation of risk management activities by Parties to the MOU.

2.4.2 Taskforce Management Office (TMO)

The TMO is responsible for risk management coordination, maintaining the FFT Strategic Risk Register and providing support to the IDC, FFT Committees and working groups to implement effective risk management of the FFT.

OFFICIAL**Diagram 1: Fraud Fusion Taskforce Governance Framework**

2.5 Embedding risk management

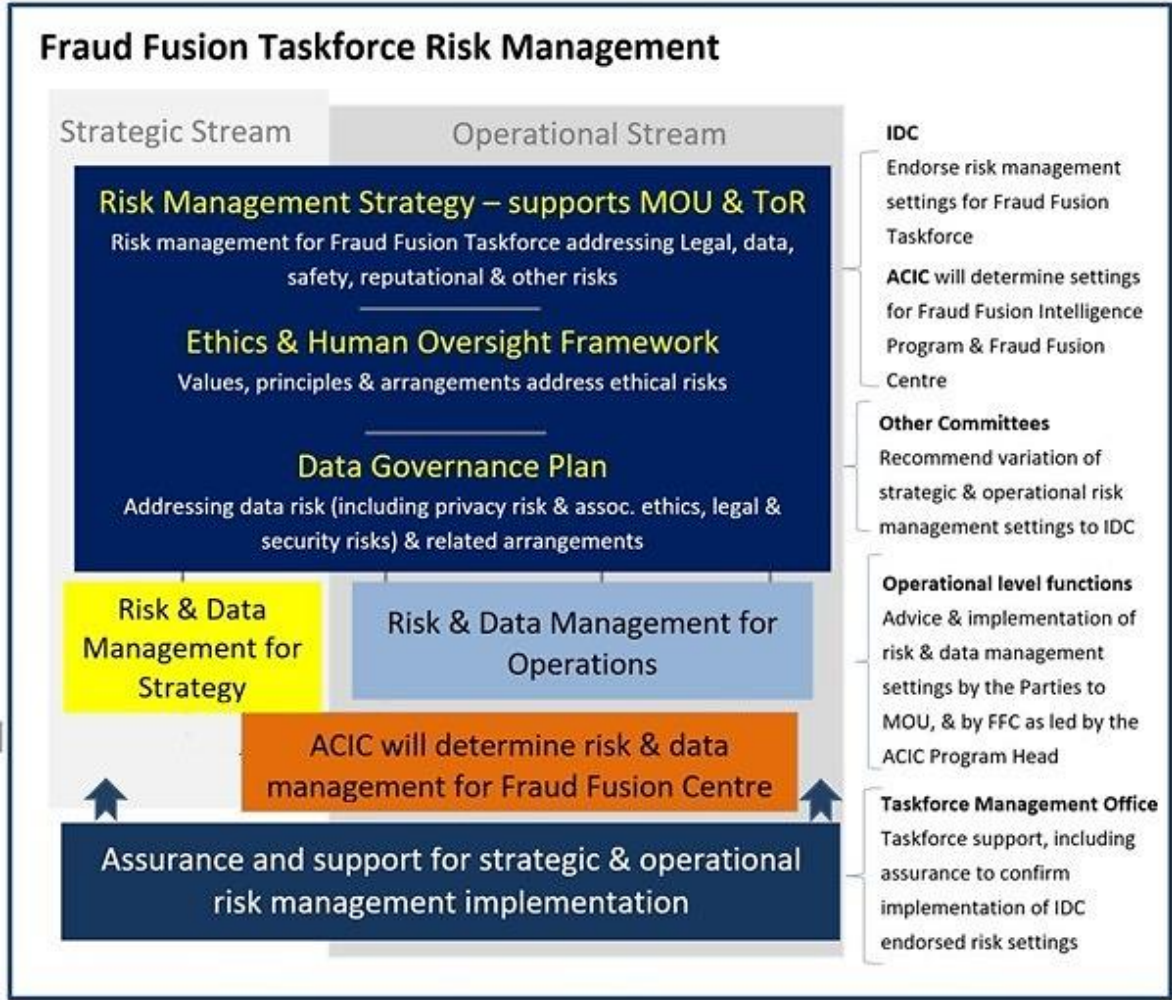
The embedding of FFT's management of risk across its activities and operations is supported by existing FFT governance and assurance frameworks and business processes including:

- FFT Communications and Engagement Strategy
- FFT Ethics and Human Oversight Framework
- FFT Data Governance Framework and Fraud Fusion Centre Data Governance Plan
- FFT Reporting Framework
- FFT Evaluation Framework
- FFT Prioritisation Framework and Case Catalogue.

OFFICIAL

Operational risk management policy and procedures by respective Parties of the MOU that affect FFT integrated strategic risk management.

Diagram 2: Fraud Fusion Taskforce Risk Management Framework visual



2.6 Roles and Responsibilities

The *Public Governance, Performance and Accountability Act 2013* (PGPA Act) requires each agency to establish and maintain systems relating to risk and control. The FFT Risk Management Strategy identifies roles and responsibilities of key positions in the FFT. Key roles and responsibilities for the management of material shared risks (strategic, operational and tactical) in relation to FFT activity are set out in the following table.

OFFICIAL**Table 1: Roles and Responsibilities for FFT Risk Management**

GROUP	ROLE AND RESPONSIBILITIES
Party to the MOU	- Ensures effective risk management in respect of the scope of the FFT, and in relation to their legislative obligations, programs and shared risks. - Liaises with the TMO on shared risks and individual agency risks where relevant.
Inter-Departmental Committee (IDC)	- Overall responsibility for establishing and maintaining the FFT's risk management framework and owner of risk artefacts. - Responsible for oversight of integrated risk management of FFT shared strategic risks. - Considers risks as part of Taskforce planning processes. - Receives reporting on the control environment for strategic operational and tactical risks and risk mitigation plans. - Demonstrates and promotes a risk management culture. - Notifies higher authorities of risk matters where appropriate. (s9 PGPA Act) - Where appropriate, nominates senior personnel from participating FFT agencies to represent their agency on the FFT governance risk activities.
Strategic Prevention Committee (SPC)	- Supports the IDC and IOC in identification and management of strategic risks and influences relevant to the FFT, including fraud related risks that impact on participant safety and service quality. - Considers risks relating to forward-looking strategy referred by the IOC or the IDC and agreeing strategies to address these risks.
Intelligence and Operations Committee (IOC)	- Manages FFT shared operational and intelligence risks in accordance with IDC risk settings. - Responsible for overseeing relevant registers and reports on FFT operational and intelligence risks to IDC (and to SPC as appropriate).

OFFICIAL

GROUP	ROLE AND RESPONSIBILITIES
Taskforce Management Office (TMO)	• Supports the Parties and FFT Committees to implement effective risk management. • Risk management coordination, advice, and tools on effective risk management practice. • Maintains FFT strategic risk register and reporting process. • Provides risk assessment and reporting templates and tools. • Supports the review of the risk management framework, settings and practice to determine if risks are effectively managed by the FFT.

3. Positive Risk Culture

Risk culture refers to the shared attitudes, values and behaviours that characterise how the FFT considers risk in its decisions, actions and operations. All FFT staff have a responsibility to practice active risk management and promote a positive risk culture. A positive risk culture promotes an open and proactive approach to managing risk. It balances both threat and opportunities and empowers staff to appropriately identify, assess, communicate and manage risk.

4. Risk Appetite and Tolerance

Risk appetite is the amount of risk an entity is willing to accept or retain to achieve its objectives. The IDC has set the FFT's appetite for risk as **low (conservative)**. The FFT's risk appetite will be reviewed and set by the IDC annually.

A conservative appetite means that the time limited multi-agency Taskforce is cautious in its approach to risk and must closely monitor and regularly review how risks are managed while pursuing operational opportunities and strategic innovation to prevent and reduce fraud and criminal activity within and against Government Payment Programs through engagement and collaboration.

Risk tolerance is the level of risk taking acceptable to achieve a specific objective or manage a category of risk. It represents the application of risk appetite. Risk owners will assess each strategic shared risk and determine tolerance for the risk per the risks management process in section 5. A risk tolerance scale will be developed for each specific risk and will be in the FFT Risk Management Guide.

OFFICIAL

The FFT must closely monitor and regularly review material shared risks, and how these are managed. Risks rated as 'High' or above must be escalated to and monitored by the IDC.

4.1 Variations in Risk Rating and Tolerance

If a risk rating is higher than the risk tolerance within the FFT Strategic Risk Register, the IDC must consider this variation and if accepted, both the agreement and risk treatment must be documented, monitored and regularly reported on until the risk rating is reduced to an acceptable level (where possible).

5. Risk Management Process

The FFT Risk Management Strategy is designed to support the implementation of holistic risk management that ensures strategic, operational and tactical risk management associated with FFT activities and operations are integrated.

5.1 FFT Risk classification

The FFT classifies its material shared risks into the following categories:

- **Strategic risks** –risks that relate to the achievement of the purpose and objectives of the FFT and which may affect the strategic intent of the FFT. They may eventuate outside of the FFT's control with consequences for the FFT achieving its purpose and objectives.
- **Operational risks** – risks that relate to FFT's operations and involve people, systems and processes and within the FFT's control.
- **Tactical risks** - risks that relate to specific operational initiatives or projects implemented under the FFT and within the control of the participating agencies.

5.1.1 FFT Strategic Risk Categories

- Governance (Strategy, FFT Stakeholder Relationships)
- Operational (Participant and Customer Safety, Workforce, Data & Technology and FFT systems & processes)
- Legal
- Financial
- Reputational

5.2 FFT Shared Risk

OFFICIAL

In accordance with Element 6 of the Commonwealth Risk Management Policy, shared risks are those that extend beyond the control and visibility of a single entity and require a collaborative effort of shared oversight and management. The FFT engages in inter-agency or cross- jurisdictional activities and operations that involve risks which extend across entities.

Shared risks have some distinguishing features. They may not have an obvious owner, may be more complex because they might be influenced by multiple parties and if realised can impact different agencies in different ways.

In this context, shared risks exist where two or more Parties and/or the FFT lead agencies are exposed to and/or can significantly influence risk (i.e. inter-dependent risk) held by one or more Parties because of involvement in the FFT. The FFT will identify, assess, and manage shared risk at strategic and operational levels. The management of FFT shared risks should be agreed on by relevant Parties of the MOU involved and documented in the FFT Strategic Risk Register.

Management of shared tactical level risk ('FFT tactical risk') will be separately addressed between/by specifically involved agencies on a case-by-case basis. Risk assessment and control monitoring will inform integrated shared risk management, including from agencies responsible for FFT shared tactical risk.

Each Party to the MOU will at all times remain accountable to ensure effective risk management of shared risks in relation to their agency's legislative obligations, and enterprise risks associated with their agency's business activities and programs.

OFFICIAL**Diagram 3: FFT Integrated Shared Risk Management**

5.3 Management of FFT Shared Risk

5.3.1 Shared Risks

Government payment and program specific risks and risks to program stakeholders that arise for two or more Parties to the MOU due to the FFT, that are shared or inter-dependent with another Party will be recorded in the FFT Strategic Risk Register and management will be actively reviewed by the FFT (considered 'shared risks'). These risks include the risk that private, confidential, sensitive data/information is leaked/accessed for unintended or malicious purposes.

Risk that arises due to the commencement and operation of the FFT, that is not program or payment specific but are shared by the Parties to the MOU, will also be addressed in the FFT Strategic Risk Register. For example, the risk that FFT planning and engagement between Parties is inadequate and therefore governance and operational activity will not meet the purpose and objectives of the FFT.

OFFICIAL

For each shared risk in the FFT Strategic Risk Register, a principal risk owner of the shared risk should be nominated, that is the member of IDC whose agency has the principal responsibility for the shared risk. Other agency risk owners that share the risk to some degree should also be nominated in the corresponding section of the FFT Strategic Risk Register. [Comcover guidance](#) is available to support the management of FFT shared risks.

5.3.2 Non-shared risks

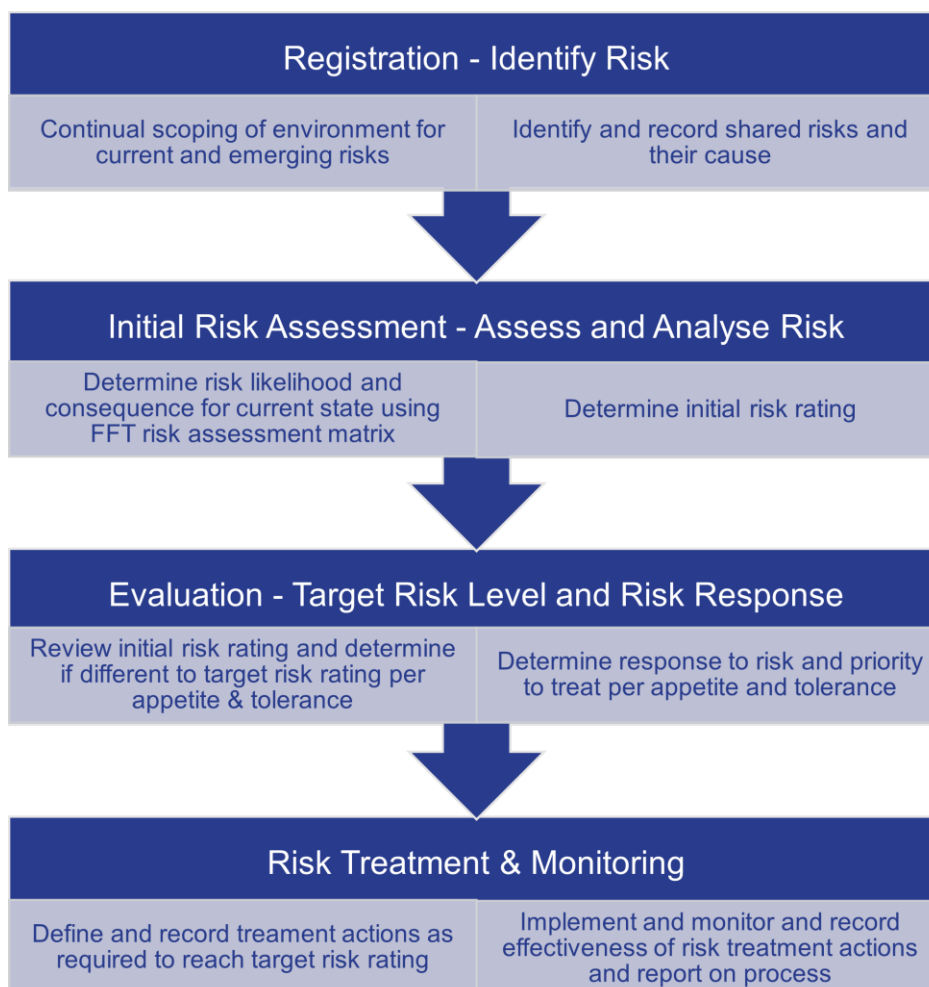
Risks that are not shared or impacted by another Party to the MOU, or their action/inaction, will be managed by each respective Party. This will occur under that agency's own governing risk management and regulatory framework with appropriate regard to the MOU and Terms of Reference.

5.4 FFT Risk Management Process

The FFT's risk management process includes risk and issue identification, assessment and analysis of risk (to assign a risk rating), evaluation and treatment of risk (to assign treatment and ownership), and ongoing monitoring and reporting of both shared risks and issues.

Guidance on the FFT risk management process is outlined in the FFT Risk Management Guide.

The FFT's risk management cycle is outlined in the diagram below.

OFFICIAL**Diagram 4: FFT Risk Management Process****5.4.1 FFT Risk Registers**

Risks that impact FFT activities, operations and decisions will be documented and managed through regular review of the FFT Strategic Risk Register by the IDC.

Specific risk registers should be developed for FFT governance committee activity and projects and where necessary for any tactical operations to capture the scope and nature of risks involved. For example, any specific cross-agency operations which will be managed by the relevant Parties of the MOU leading the operation. Copies of specific FFT risk registers should be provided to the TMO regularly.

The Strategic Risk Register assigns control owners for each strategic risk. Operational Registers will assign control owners of operational and tactical risks. Individual agencies will manage FFT related risks through their own agency risk registers. Individual agency owners can only be responsible for the risk as it applies within their own agency.

OFFICIAL**Table 2: Assigned roles and responsibilities on FFT risk registers.**

Role	Responsibilities
Risk owners	- Responsible for overseeing end-to-end management of one or more individual risks once nominated as a 'risk owner' on a risk register. - Outline risk treatment, including treatment and control ownership in risk treatment plans. - Accountable for monitoring, reporting and escalating risks.
Treatment owners	- Responsible for overseeing effective treatment of one or more individual risks once nominated as a 'treatment owner' on a risk register. - Reporting to risk owner on treatment implementation and effectiveness for subject risk/s and related issues
Control owners	- Responsible for implementing and maintaining effective controls, including assessing and monitoring their effectiveness once nominated as a 'control owner' on a risk register. - Reporting to treatment owner on control performance and effectiveness for subject risk/s and related issues.
Influencing Agency	An agency that may be identified as influencing the likelihood or level of impact for one or more other Parties of a risk occurring (this agency may not be impacted should the risk occur).

6. Managing the Framework

6.1 Reporting

The *Public Governance, Performance and Accountability Act 2013* (PGPA Act) requires each agency to establish and maintain systems relating to risk and control. Timely and accurate reporting is essential to monitoring the FFT's performance to ensure:

OFFICIAL

- FFT will follow the principles of the PGPA Act in its approach to risk management.
- FFT Committees can maintain appropriate oversight of FFT activities and operations.
- FFT can appropriately manage all risks including emerging and ethical risks and
- FFT is complying with its Frameworks.

The FFT Reporting Framework has framework assurance and risk reporting requirements. FFT framework and assurance and risk reporting may be used for annual reporting purposes and at the discretion of the FFT.

6.1.1 FFT Framework Assurance Reporting

The TMO will coordinate FFT assurance activities to monitor compliance with FFT Frameworks and Registers. This includes compliance with the Risk Management Framework. This will ensure the IDC has effective oversight and can monitor the successful implementation of the Framework.

The quarterly assurance process will include the FFT Committees and working groups providing documented risk information to the TMO for review. This information will inform the assurance reporting dashboard. The TMO will prepare an assurance reporting dashboard for quarterly reporting to IDC.

6.1.2 FFT Risk Reporting/Escalation

FFT Committees, working groups and FFT member agencies provide oversight on specific areas of FFT strategy and operations and are responsible for identifying and managing risks including emerging risks.

All risks including emerging risks should be documented on FFT operational registers. Risks including emerging risks that require escalation to IDC should be communicated to the TMO for recording on the FFT Strategic Risk Register. Risks rated as 'High' or above must be escalated to and monitored by the IDC.

Risk reporting to IDC will occur quarterly through the FFT Strategic Risk Register and Risk Dashboard.

The FFT Strategic Risk Register will be provided to IDC to discuss and determine:

- any identified risks that impact FFT operations, and recommend treatments
- any emerging risks raised by FFT member agencies and

OFFICIAL

- whether identified risks sit on FFT Strategic Risk Register, or the relevant operational risk register or both registers concurrently.

6.2 Post implementation Review

The FFT is committed to continuous improvement.

Consistent with Element Nine of the Commonwealth Risk Management Framework, the FFT Risk Management Strategy will be reviewed at least annually to ensure controls continue to be relevant, effective and address emerging risks including substantial changes in the FFT's structure, functions or activities.

This will ensure that:

- The FFT Risk Management Strategy and FFT Strategic Risk Register reflects the FFT's operating environment.
- Risk management processes continue to be effective.
- Reporting continues to provide information necessary to enable delegates to make informed decision making, maintain appropriate oversight, and enable continuous improvement; and
- Risk management continues to effectively contribute to delivering the FFT's purpose and objectives.