Australian Government
Commonwealth Superannuation Corporation

Fraud, Scams and Corruption Control Plan

2025

CSC
Commonwealth Superannuation Corporation

Document and version control

Version No	Date	Comment	Preparer	Reason for change
1.0	02/05/2013	Board Approved Plan	Andy Young, General Manager Finance & Risk	Annual review
2.0	19/08/2014	Board Approved Plan	Andy Young, General Manager Finance & Risk	Annual Review
3.0	26/08/2015	Board Approved Plan	Andy Young, General Manager Finance & Risk	Annual Review
3.1	06/2016	Board Approved Plan	Andy Young, General Manager Finance & Risk	Annual review, integration and recommendations from external consultant
4.0	25/07/2017	Board Approved Plan	Rob Firth Head of Risk	Annual Review
4.1	04/06/2018	Board Approved Plan	Rob Firth Head of Risk	Annual Review
5.0	21/11/2019	Board Approved Plan	Rob Firth Chief Risk Officer	Annual Review
5.1	23/09/2020	Board Approved Plan	Rob Firth Chief Risk Officer	Annual Review
5.2	18/11/2021	Board Approved Plan	Rob Firth Chief Risk Officer	Annual Review
5.3	15/09/2022	Audit Committee Approved Plan	Rob Firth Chief Risk Officer	Annual Review
6.0	23/08/2023	Board Approved Plan	Mark Brogan Senior Manager, Risk (FCCO)	Annual Review
7.0	21/08/2024	Risk Committee Approved Plan	Mark Brogan Senior Manager, Risk (FCCO)	Annual Review
8.0	05/08/2025	Revised to include scams response	Mark Brogan Senior Manager, Risk (FCCO)	Annual Review

Table of Content

1 Executive summary

1.1 Introduction

Commonwealth Superannuation Corporation ('CSC') recognises safeguarding the assets of member funds, Commonwealth monies and CSC itself against loss by fraud or having any connection to corruption, is a key responsibility of all employees[1]. All employees are required to implement and adhere to fraud and corruption control procedures and the reporting of all instances of suspected fraud and corruption.

CSC recognises it has a responsibility to develop and implement sound financial, legal and ethical decision-making and practices. The purpose of this document is to outline CSC's plans for controlling the risk of fraud and corruption. This Fraud, Scams and Corruption Control Plan forms part of the risk management framework of CSC and is complemented by other elements of CSC's risk management framework, particularly the Audit Committee, Risk Committee, its Risk Management Strategy, Risk Appetite Statement and internal process and procedure documents. The Fraud, Scams and Corruption Control Plan has been extended to cover CSC's response to member scams.

This Fraud, Scams and Corruption Control Plan and the ongoing fraud and corruption program represent CSC's commitment to the management and control of fraud and corruption. Any references to 'CSC' in this Plan are taken to be references to CSC, the funds for which CSC acts as trustee and the Commonwealth monies to which CSC has access as part of administering member benefits and pensions.

1.2 Statement of Attitude to Fraud, Scams and Corruption

CSC recognises external fraud may occur across its member base and is committed to minimising the incidence and consequences of these events through a risk management approach, which incorporates prevention, detection and response strategies.

1.3 Approach

This Fraud, Scams and Corruption Control Plan aims to draw together all prevention, detection and response initiatives adopted by CSC in one document and, more specifically, to:

- Promote the awareness of risks relating to fraud, scams and corruption to the Board, Audit Committee, Risk Committee, management and staff
- Develop appropriate strategies and internal controls to minimise losses due to fraud, scams and corruption to CSC
- Address material fraud risks identified by CSC as articulated within the overall risk register.

1.4 Australian Standards, Prudential Guides and Public Sector Guidelines

This Fraud and Corruption Control Plan aligns with the following Australian Standards:

- AS 8001-2021 – Fraud and Corruption Control
- ASFA Best Practice Paper No. 20 Managing the risk of fraud and corruption in superannuation funds
- APRA SPG 223 – Fraud Risk Management
- Commonwealth Fraud Control Framework

[1] *For the purposes of this policy an employee of CSC includes Directors, staff and also contractors*

1.5 Definitions

For the purposes of the Fraud, Scams and Corruption Control Plan, CSC has adopted the following definition of fraud:

*Dishonest activity causing actual or potential gain or loss to a person or organisation including theft of moneys or other property by persons internal and/or external to the organization and/or where deception is used at the time, immediately before or immediately following the activity. (*Ref. AS8001-2021 1.4.8 *)*

- Property in this context also includes intellectual property and other intangibles such as information
- Fraud also includes the deliberate falsification, concealment, destruction or use of falsified documentation used or intended for use for a normal business purpose or the improper use of information or position for personal financial benefit
- While conduct must be dishonest for it to meet the definition of "fraud" the conduct need not necessarily represent a breach of the criminal law
- The concept of fraud within the meaning of this Standard can involve fraudulent conduct by internal and/or external parties targeting the organization or fraudulent or corrupt conduct by the organization itself targeting external parties

For the purposes of the Fraud, Scams and Corruption Control Plan, CSC has adopted the following definition of member scams:

Scams are a sub-set of fraud where people are tricked into providing information or money. CSC's definition is narrower and limited to situations where members authorised a transaction by either making the transaction or aiding the scammer to make the transaction, including by providing Multi-Factor Authentication (MFA) passwords. This is differentiated from the broader definition of scams where the customer provided the scammer with personal information (such as date of birth, and address) allowing them to impersonate the member and conduct the unauthorised transaction.

1.5.1 Internal Fraud

Internal fraud relates to where an employee is involved.

Common examples of internal fraud include:

- Unauthorised payment or redirection of funds
- Disclosing confidential information for financial or non-financial gain
- Fraud against member entitlements
- Misuse of position
- Misuse or unlawful use of resources

Common indicators for internal fraud (Red Flags) might indicate an employee:

- Living beyond their means
- Having financial difficulties
- Being overly defensive or having a suspicious attitude
- Demonstrated behavioural changes – this may be an indication of drugs, alcohol or gambling
- Having prior fraud convictions
- Unwillingness to disclose or share duties

1.5.2 External Fraud

External fraud relates to activities committed from outside CSC, e.g. by scheme members, clients, service providers or members of the public.

Common examples of external fraud include:

- Falsifying or omitting information on a claim form to obtain a benefit
- Online account takeover or improperly changing bank account and other details
- Impersonating a member (Identity Fraud)
- Cybercrime (online scams, attacks on computer systems or websites)

Common indicators for external fraud (Red Flags) may include:

- Struggling to answer your questions or guessing (i.e. previous employer, contributing status etc.)
- Being overly impatient or threatening to complain
- Attempting multiple benefit claims
- Phishing for proof of identity (POI) information
- Unnecessary reinforcing or being overly repetitive of specific information
- Attempting to be overly familiar.

1.5.3 Corruption

Corruption is defined as:

*Dishonest activity in which an employee within an organisation acts contrary to the interests of the organisation and abuses their position of trust in order to achieve personal advantage or advantage for another person or organisation. This can also involve corrupt conduct by the organisation, or a person purporting to act on behalf of and in the interests of the organisation, in order to secure some form of improper advantage for the organisation either directly or indirectly. (*Ref. AS8001-2021, 1.4.8*)*

Corruption may include but is not limited to:

- Making or receiving a payment that determines the outcome of a transaction (bribery).
- Paying or receiving secret commissions or kick backs
- Undue influence in the selection of a service provider who is connected in some way to the influencer
- Making payments to a third party to obtain unfair competitive advantage.

Common indicators for corruption (Red Flags) may include:

- Goods, services, jobs, and sometimes scholarships provided to persons connected to the influencer / decision maker
- Unusually close association with vendor/supplier
- Last minute roadblocks requiring additional payments to “get the transaction over the line”
- Transacting counterparty may not be identified or may be changed at the last moment
- An employee being overly guarded on transaction arrangements
- An employee being reluctant to explain certain costs or fees
- Costs / fees for unnecessary activities
- Lack of clarity on actual goods / services received.

1.5.4 Facilitation Payments

A facilitation payment is a payment made to expedite an administrative process. A facilitation payment does not 'determine' the outcome of a transaction (as this would be a bribe).

1.6 Related policies and documents

- Risk Management Strategy and Risk Appetite Statement
- Anti-Money Laundering and Counter Terrorist Financing Program
- Whistle-blower Protection and Public Interest Disclosure Policy
- CSC Code of Conduct
- IT Security and Acceptable Usage Policy
- Conflicts Management Policy and Framework
- Outsourcing Policy
- Fit and Proper Policy
- Privacy Policy
- ICT Information Management Policy
- ICT Security Policy
- CSC Personnel Security Policy.

1.7 Scope

This Plan applies to the prevention, detection and response to fraud, scams and corruption incidents at or involving CSC whether they are due to the actions of employees, service providers, members or other external parties.

1.8 Structure

CSC has committed to fraud and corruption control by developing the Fraud, Scams and Corruption Control Plan. The Fraud, Scams and Corruption Control Plan details the strategies in place to manage the risks of fraud and corruption and is structured in four sections:

a) Planning and resourcing – to implement the Fraud and Corruption Control Plan

b) Prevention – controls designed to reduce the risk of fraud and corruption occurring

c) Detection – controls designed at detecting fraud and corruption as soon as possible if it does occur

d) Response - controls designed to ensure any fraud and corruption detected is investigated thoroughly and appropriate action taken.

The Fraud, Scams and Corruption Control Plan also details how CSC will implement and monitor these initiatives.

2 Planning and resourcing

2.1 Fraud, scams and corruption control responsibilities

Fraud and corruption control responsibilities are outlined below and summarised in Appendix A – Fraud and Scam responsibilities.

2.1.1 Board

The Board is the governing body and is ultimately accountable for the management of fraud, scams and corruption risks. This includes the approval of and monitoring the progress of this Plan. The Board also;

- Acknowledges fraud, scams and corruption as a serious risk
- Has an awareness of the CSC's fraud, scams and corruption exposures; and
- Demonstrates a high level of commitment to controlling the risks of fraud, scams and corruption both against CSC and by CSC.

2.1.2 Risk Committee

The Risk Committee is responsible for oversight of the fraud, scams and corruption risk management program. This includes recommending the Fraud, Scams and Corruption Control Plan to the Risk Committee for recommendation to the Board for approval. The Risk Committee will be notified of reports of fraud, scams and corruption and the related investigations. The Risk Committee will have a regular agenda item for fraud, scams and corruption reporting and will receive an annual summary report of all fraud, scams and corruption incidents. The Risk Committee will receive updates on the status of fraud, scams and corruption risk assessments and will ensure key fraud, scams and corruption risks are addressed in the annual internal audit plan.

2.1.3 Fraud and Corruption Control Officer

The Fraud and Corruption Control Officer ('FCCO') is responsible for the coordination and ongoing monitoring of the fraud, scams and corruption risk management program as documented in Appendix A – Fraud and Scam responsibilities. CSC has appointed the Senior Manager, Risk as the FCCO (and in his absence the Chief Risk Officer). The FCCO reports to the Chief Risk Officer and the Risk Committee on matters concerning the Fraud, Scams and Corruption Control Plan. Refer to Appendix C – Contact details.

The FCCO is responsible for periodic reporting to the Risk Committee on all matters concerning fraud, scams and corruption risk management within CSC. This includes reporting on fraud, scams and corruption reports and related investigations, presenting an annual summary report of all fraud, scams and corruption incidents and providing updates on the status of fraud, scams and corruption risk assessments. The FCCO is also responsible for reviewing the Fraud, Scams and Corruption Control Plan on an annual basis. The FCCO is assisted in their duties by the Fraud Risk Analysts.

2.1.4 Investigations

The Fraud Risk Analyst is responsible for undertaking preliminary investigations of allegations of fraud and taking appropriate actions to investigate and report on that fraud as appropriate. The Fraud Risk Analyst will report on the outcome of all preliminary fraud investigations to the FCCO.

External parties engaged to assist in investigations on CSC's behalf shall enter into a binding agreement in relation to the release of confidential information coming into their possession during the course of the investigation. (Ref. AS8001-2021, 5.3.5)

2.1.5 Senior management

Senior management must demonstrate their commitment to controlling the risks of fraud, scams and corruption by ensuring they, and their staff, adhere to the requirements of the Fraud, Scams and Corruption Control Plan and assisting in implementing the documented risk management strategies. This includes ensuring they and their staff attend training, contribute to the completion of fraud, scams and corruption risk assessments, adhere to internal controls and report any concerns via the reporting mechanisms.

2.1.6 Line management

Line management must demonstrate their commitment to controlling the risks of fraud, scams and corruption by ensuring they, and their staff, adhere to the requirements of the Fraud, Scams and Corruption Control Plan and assisting in implementing the documented risk management strategies. This includes ensuring they and their staff attend training, participate in the fraud, scams and corruption risk assessments, adhere to internal controls, and implement control enhancements. Line managers must also escalate relevant matters in accordance with FCCP.

2.1.7 Employees

All CSC employees have a responsibility to:

- Adhere to the requirements of the Fraud, Scams and Corruption Control Plan
- Act in accordance with the CSC Values and Code of Conduct including notification of any conflict of interest
- Assist in the implementation of the strategies documented in the Fraud, Scams and Corruption Control Plan
- Assist with all reports of fraud or improper conduct in a professional and prompt manner. Employees with specific responsibilities for a fraud and corruption control detailed in their role descriptions and performance plans must adhere to these responsibilities.

2.1.8 Internal Audit

While primary responsibility for the identification of fraud within an organization rests with management, the internal audit function can, in the context of addressing business risks, be an effective part of the overall Plan to identify, prevent and detect fraud and corruption. (Ref. AS8001-2021, 2.11.1)

The internal auditors are responsible for:

- providing assurance to the Audit Committee & Risk Committee on the effectiveness of the internal controls in place to mitigate risks
- providing an independent opinion on the management of risks
- developing the annual internal audit plan based on identified key risk areas
- timely reporting any instances of fraud or corruption detected and related weaknesses in controls

The Audit Committee and Risk Committee will provide Internal Audit reference to the material fraud and corruption risks identified in the material risk register when developing the annual internal audit plan.

2.1.9 CSC Contact Centre

Contact centre employees have an ongoing requirement to be vigilant in relation to fraud and corruption and respond accordingly. This includes recording all allegations coming into the Contact Centre, directing to the appropriate business area if the allegation is in the nature of a query or complaint, and referring allegations of genuine concern for investigation.

3 Prevention

Preventative controls are designed to reduce the risk of fraud, scams and or corruption from occurring. CSC's first line of defence approach to fraud, scams and corruption prevention includes building and maintaining high integrity and a strong culture within the organisation.

3.1 CSC – Code of Conduct

The CSC Code of Conduct provides employees with guidance on appropriate ethical standards for work related behaviour.

3.2 Fraud, scams and corruption risk assessment

The Fraud, Scams and Corruption Risk Assessment ('FCRA') will be conducted at least once every two years (as part of the internal audit plan) or more frequently if a material change in CSC's operations has occurred in the opinion of the FCCO. The FSCRA will be coordinated by FCCO and the results and the status on the implementation of the proposed actions arising from the FSCRA will be reported to the Risk Committee. Each business area of CSC is also responsible for the identification and management of risks within its own area of responsibility and notifying the FCCO of any updates or amendments to the FSCRA. The FCCO is also required to review any new or revised operations or initiatives to ensure fraud, scams and corruption risks are adequately considered.

The FSCRA will be conducted in accordance with CSC's Risk Management Strategy and Risk Appetite Statement, ISO 31000:2018 *Risk Management-Principles and Guidelines* and AS 8001 – 2021.

3.3 Fraud and corruption awareness

The primary purpose of fraud, scams and corruption awareness training is to assist in the prevention of fraud, scams and corruption by raising the general level of awareness amongst all employees and to ensure they are aware of how to report suspicions.

New employees will receive a mandatory fraud, scams and corruption awareness training at induction. The FCCO, with assistance from Executive Managers[2], will identify whether employees are considered to be working in high-risk roles require additional training.

The FCCO will be responsible for ensuring training materials are reviewed concurrently with the review of the Fraud and Corruption Control Plan.

3.4 Employee due diligence

CSC performs pre-employment screening processes on all employees including:

- identity verification
- confirmation of all relevant professional and tertiary qualifications
- independent reference checks
- criminal history check
- declaration of any conflicts of interest (including supplier or adviser relationships) post August 2018

[2] For the purposes of this system Executive Mangers include all Executive Managers, Chief Operations Officer, Chief Investments Officer and Chief Customer Officer.

Consideration will also be given to other checks as required and determined by the level of risk associated with an individual's position such as confirmation of professional memberships, media searches, directorship and shareholding searches, civil proceedings and work rights status.

Employee Due Diligence checks may be re-performed (if requested). CSC's Responsible Persons (as defined by APRA) are required to complete an annual certification and undergo a criminal history check every 3-5 years.

3.5 Conflicts of interest

Employees must report in the CSC Gifts and Conflicts Register any conflicts of interest, whether actual, potential or perceived, and any gifts and other interests received. Employees must:

- not make decisions, particularly regarding scheme benefits and entitlements, which relate to co-workers, family members, friends or persons with whom they have a close personal relationship
- obtain written approval from their manager prior to commencing other employment, including self-employment or a business, while an employee of CSC
- not use information not publicly available for personal gain
- maintain appropriate records of dealings in securities, and provide a copy of these records if requested by the Board of Directors.

3.6 Third party due diligence

CSC's Supplier Management Policy sets out the key processes and procedures CSC applies in relation to the outsourcing of material business activities to external service providers. Wherever possible, CSC follows these processes with all outsourcing. Refer to the CSC's Supplier Management Policy for more information.

3.7 Internal controls

CSC's internal control environment includes controls that assist in the prevention of fraud, scams and corruption including authorisation and approvals, documented operating procedures, access restrictions and segregation of duties. Specific controls in place to prevent fraud, scams and corruption are articulated in the Material Risk Register.

3.8 Pressure Testing the Internal Control Plan

Pressure testing involves an internal or external individual or team initiating a series of test transactions to assess the operational effectiveness of internal controls. This involves the introduction of documents, data or other action consistent with an actual fraud or corruption event, to determine if existing internal controls are operating as intended and are effective in preventing fraud, scam or corruption of the type contemplated, and then observing how existing internal controls respond to such a test transaction. Examples of actions that can be used include submitting a 'false' invoice for payment, email communication to change the bank account details of a supplier or a telephone call to change the contact details of a client. (Ref. AS8001-2021, 3.5.3)

CSC shall ensure that internal controls improvements identified by the pressure testing program are remediated.

Common vulnerabilities that can be uncovered through pressure testing include the following:

- A lack of fraud awareness.
- Inadequate quality assurance.
- Not verifying information or evidence.
- A lack of effective oversight.
- Inadequate technology controls.
- Inadequate detection controls.
- A lack of reporting or reconciliation.

4 Detection

CSC recognises, despite a comprehensive fraud control program, it is nevertheless possible that fraud, scams and corruption may still occur. Accordingly, CSC has adopted strategies aimed at detecting fraud, scams and corruption as soon as possible after it has occurred. Line management should be alert to new fraud, scams and corruption risks and discuss additional detection controls with the FCCO.

The specific controls CSC has in place are detailed in the FSCRA. Holistic fraud, scams and corruption controls are described below.

4.1 Detection mechanisms

4.1.1 Post-transaction review

A review of transactions (reconciliations) after they have been processed can be effective in identifying fraudulent activity, such as uncovering altered or missing documentation, falsified or altered authorisation or inadequate supporting documentation.

4.1.2 Data analytics

CSC's data is a critical source of information for detecting potential fraud, scams or corrupt conduct. By the application of sophisticated analytical techniques, a series of indicators of fraud, scams and corruption can be identified and then investigated.

Data analytic tests shall capture relevant indicators of fraud, scams or corruption exposures. A consideration of how most effectively and efficiently data analytics will be applied to the task of identifying possible fraud and corruption events include a detailed consideration of the software to be used. By the application of software applications and techniques, a series of suspect transactions can be identified and then investigated thus potentially detecting fraudulent or corrupt conduct at an early stage. (Ref. AS8001-2021, 4.5)

4.1.3 ICT[3]/Cyber Security Controls

CSC implements and maintains ICT security controls which protects us from external cyber-attacks. Some examples include:

- Anti-malware
- Intrusion detection
- Network analytics

Refer to the Information Security Management Policy and ICT Security Policy for more information.

4.1.4 Strategic analysis of management accounts

CSC analyses management accounting reports for budgetary purposes and this may also identify transactions or trends indicative of fraudulent or corrupt conduct. Some examples of management reports analysed are:

- actual expenditure against budget for individual cost centres
- reports comparing expenditure against prior periods.

[3] Information and Communications Technology (ICT).

4.1.5 Exit Interviews

Exit interviews provide employees the opportunity to disclose their motivation for leaving CSC. If anything suspicious comes to the interviewer's attention, it will be reported to the FCCO.

4.2 Internal Audit program

As the third line of defence, Internal Audit function provides an important risk assurance function by testing the effectiveness of controls designed to prevent fraud, scams and corruption but, it is also useful in the detection of fraud. The FCCO will assist, through the Annual Internal Audit Plan (endorsed by the Audit Committee), that Internal Audit resources are applied to provide the appropriate focus on detecting fraud against CSC.

4.3 External Audit

Although the activities undertaken by external auditors has a preventative benefit, they also have an important role in fraud, scams and corruption detection. The external auditors are required to review and express an opinion on the accuracy of CSC's financial statements. Although not their primary objective, they may identify fraud, scams or corruption and must report this to the Audit Committee. In performing their work, they also form a view on the effectiveness of internal controls including those relating to the risk of fraud, scams and corruption.

4.4 Fraud and corruption reporting

All employees and service providers are required to immediately report any suspected, attempted or actual fraud, scams or corruption incident. Members and the general public are also encouraged to make reports directly to CSC.

Reports may be made to:

- A supervisor or manager
- The Fraud Risk Analyst or if the Fraud Risk Analyst is unavailable or implicated in the report, the FCCO
- The Internal Fraud Control hotline/email
- The Contact Centre (for member or scheme related fraud referrals)
- The External Fraud Control email (on scheme and corporate external websites).

This reporting framework is summarised Appendix B.

The information provided for any allegation of fraud should include:

- a description of the suspected fraudulent or scam conduct
- details of any employee, fund member or external parties involved (name and location)
- the value of the alleged fraud, scam or improper conduct
- potential sources of additional information about the matter in question, such as people and files.

Eligible whistleblowers can make whistleblower disclosures and/or public interest disclosures. If whistleblowers wish to seek protection, then they must follow the processes outlined in CSC's Whistleblower Protection and Public Interest Disclosure Policy.

As set out in the Whistleblower Protection and Public Interest Disclosure Policy, any person may refer a corruption issue or provide other information about a corruption issue to the National Anti-Corruption Commission (NACC).

Individuals should not attempt to conduct any investigation activities. Anonymous reports can be made to the Fraud Control hotline/email.

It is a breach of this Plan to attempt to prevent an employee from making a report under this Plan.

4.5 Protection of employees reporting suspected fraud

CSC will endeavour to protect employees from any form of recrimination or reprisal after they have made an allegation of fraud or corruption against another employee or external party. The protections afforded have been documented in the Whistle-blower Protection and Public Interest Disclosure Policy.

All reports are treated confidentially. Subject to legal obligations, all reports received will be held in confidence and disclosed on a 'need to know' basis. The identity of a person who is the subject of allegations or an investigation will be protected as much as practicable and in accordance with the relevant law.

CSC will ensure all employees are aware of the fraud and corruption reporting requirements and actively encourage all employees to report suspected cases of fraud and corruption through appropriate channels.

5 Response

5.1 Internal reporting and escalation

5.1.1 Escalation to the Fraud Risk Analyst and FCCO

When a supervisor or manager receives an allegation of fraud or corruption, they should refer this to the Fraud Risk Analyst as soon as possible. Where the Fraud Risk Analyst is not available or is implicated, this should be referred to the FCCO.

For reports into the Contact Centre, the Customer Engagement Representatives (CERs) should escalate initially to their respective team lead who will refer the report on to the Contact Centre Quality team as appropriate.

The Fraud Risk Analyst will, as soon as possible after receiving notification of the incident, ensure it is recorded in CSC's Governance, Risk and Compliance (GRC) system, OSCAR.

5.1.2 Escalation to the CRO, CEO, Chair, Risk Committee and the Board

For potentially significant incidents, the FCCO must be notified as soon as possible. FCCO will exercise professional judgement in deciding whether a particular event is a significant incident requiring escalation. The CEO is responsible for advising the Chair of the Risk Committee and the Board, as appropriate, of significant incidents once a prima facie case of fraud has been confirmed. The FCCO will keep the CRO informed (and CEO as appropriate) of the progress of any investigation into an allegation of significant fraud against CSC and will report the outcomes of the investigation to the CSC Risk Committee.

5.1.3 Response strategy

CSC will perform preliminary investigations. Where appropriate, external expertise may be sought to assist with an investigation. The decision to obtain such external expertise will be at the discretion of the FCCO. The external expertise will be required to be trained and comply with relevant standards, in particular around capturing, analysing and managing digital evidence (Ref. AS8001-2021, 5.3.6).

In the case of internal fraud, the Executive Manager, People will be consulted, so they can advise the appropriate process to follow for the employee or concerned party.

5.1.4 Record keeping

The Fraud Risk Analyst is responsible for documenting the decisions in relation to investigations and maintaining an appropriate record of all instances of investigated fraud, scams and corruption. The FCCO will report periodically to the Risk Committee and provide annual summaries of all reported fraud, scams and corruption incidents. Reporting will include the outcome of investigations and any remedial actions taken.

5.2 Investigation procedures

The Fraud Risk Analyst is responsible for conducting the investigation in a manner that ensures procedural fairness and natural justice and observes the rules of evidence. Details of investigations will not be discussed with anyone other than those who need to know. The Fraud Risk Analyst in consultation with FCCO will be responsible for implementing the response strategy and if required will appoint an appropriately skilled, experienced and independent manager to conduct or coordinate the investigation. CSC must comply with any 'stop action' direction issued by the NACC in relation to a corruption issue. In the event that the NACC refers a corruption issue to CSC for investigation, CSC has to follow any direction given by the NACC regarding the conduct of that investigation.

5.3 Disciplinary procedures

Any breach of employment conditions in relation to fraud or corruption will be considered as serious and disciplinary action may follow, regardless of seniority. The disciplinary process will be conducted in accordance with CSC's policies and procedures. Disciplinary action may include termination of employment.

5.4 Reports to the police

Where appropriate, if there is evidence of fraud, scams or other illegal conduct by employees or external parties, the FCCO will report the incident to police.

5.5 Referral to the NACC

CSC has mandatory referral obligations to the NACC in respect of corruption issues which are suspected of involving serious or systemic corrupt conduct. Refer to Appendix A – Fraud and Scam Responsibilities as well as the Whistleblower and Public Interest Disclosure Policy.

The NACC has compulsory information gathering powers, including to request information or documents, issue summonses and undertake searches. It is important that a recipient of a notice complies with its terms, including any non-disclosure note.

5.6 Reporting to regulators and auditors

Where appropriate or required by law, General Counsel (in consultation with the CEO) will report instances of fraud to APRA and /or ASIC and to CSC's external auditors.

5.7 Reports to other external parties

Reporting matters of apparent fraud against other external parties (e.g. Employers, Centrelink or the Department of Veterans' Affairs) shall be at the discretion of General Counsel.

5.8 Reports to the media

CSC is committed to preserving its reputation in the event of fraud, scams or corruption. The Corporate Affairs Manager, or the people acting in this capacity will assess the need for media releases in relation to the fraud, scam and corruption incident. Any media contact will be managed in accordance with CSC's media management/contact policy.

5.9 Recovery of the proceeds of fraudulent conduct

Where appropriate and cost effective, CSC will pursue the recovery of any money or property lost through fraud, scams and corruption, provided there is a strong prospect of a net benefit from such action.

5.10 Professional indemnity and combined crime insurance

CSC maintains Trustee Liability, Comprehensive Crime and Cyber Security Insurance at levels agreed by the Board. General Counsel is responsible for insurance reporting obligations.

5.11 Internal control review following discovery of fraud

In each instance where fraud is detected, the FCCO and relevant Executive Manager will reassess the adequacy of the internal control environment (particularly those controls directly impacting on the fraud incident and potentially allowing it to occur) and consider whether improvements are required. Where improvements are required, these should be implemented as soon as practicable.

5.12 Disruption

Disruption is an important concept as it is possible that CSC can know or strongly suspect that fraud, scams or corruption events are occurring and causing financial and/or non-financial loss, but it may not be possible to identify the perpetrators or to deal with them via investigation.

CSC's response to fraud, scams and corruption events in this situation should therefore be to disrupt the activity instead of, or in addition to, conducting an investigation. (Ref. AS8001-2021, 5.13)

Initiatives that can be used to disrupt fraud or corruption include:

- Increased audit activity in the business activity concerned
- Increased post-transactional review targeting in particular the transactions of concern
- Implementing additional / more rigorous internal controls such as authorization procedures, separation of duties (on a temporary or permanent basis)
- Closing down a sales / communication channel which has been the subject of continued attack
- Implementing additional identity validation requirements for new/existing customers / vendors
- Changing performance targets i.e. speed of processing customer withdrawals to allow employees to more carefully consider and identify fraud and corruption red flags, and
- Additional fraud, scam and corruption awareness training focusing on the specific fraud or corruption event being experienced.

5.13 Annual reporting requirements

In addition to the reporting of individual significant incidents of fraud (and scams), the FCCO will provide the following information to the Risk Committee annually:

- Details of all instances of proven or suspected fraud, scams and corruption
- The number of cases of fraud, scam and corruption referred to law enforcement and regulators
- A summary of the results of any completed prosecution
- The number of cases resolved using administrative remedies only (i.e. dismissal of an employee)
- The amount of monies recovered, both by administrative action and the use of the judicial process
- Whether external investigation resources have been used in carrying out the investigations
- Modifications made to the internal control environment subsequent to each fraud reported during the year (to allow the Risk Committee to assess whether internal control enhancements made will be effective in preventing fraud of that type in the future).

5.14 Review

The FCCO is responsible for reviewing this Plan:

- upon a significant change to CSC's operating environment
- following an incident of fraud or corruption where a weakness in the Plan is identified or
- at least annually

The outcome of each review will be reported to the Risk Committee.

Appendix A – Fraud and Scam responsibilities

The roles and responsibilities allocated within CSC are detailed below.

Task	Responsibility	Timing
Review the Fraud, Scam and Corruption Control Plan.	FCCO	Annually
Approve the Fraud, Scam and Corruption Control Plan.	Risk Committee	As required
Oversee implementation of the Fraud, Scam and Corruption Control Plan.	Risk Committee	Ongoing
Co-ordinate the implementation of the Fraud, Scam and Corruption Control Plan.	FCCO	Ongoing
Co-ordinate the FSCRA.	FCCO	Every two years
Review any new or revised operations or initiatives to ensure fraud, scam and corruption risks are adequately considered.	FCCO	As required
Co-ordinate fraud and scam awareness training.	FCCO	At induction of new employees and periodically for targeted employees
Ensure all fraud related policies and procedures are available to employees.	FCCO	Ongoing
Promulgation of fraud, ethics and security issues to employees through internal publications.	FCCO	As required
Co-ordination and follow-up of the FSCRA by ensuring all timetabled strategies are implemented.	FCCO	In accordance with implementation dates agreed in the FSCRA report.
Conducting pre-employment screening and background checks on all employees.	Executive Manager, People	As required
Where consultants require unsupervised access to CSC's buildings or networks, confirming with the provider that requirements under CSC's Personnel Security Management Policy (including police checks and security clearances where required) are satisfied.	Contract Managers	As required

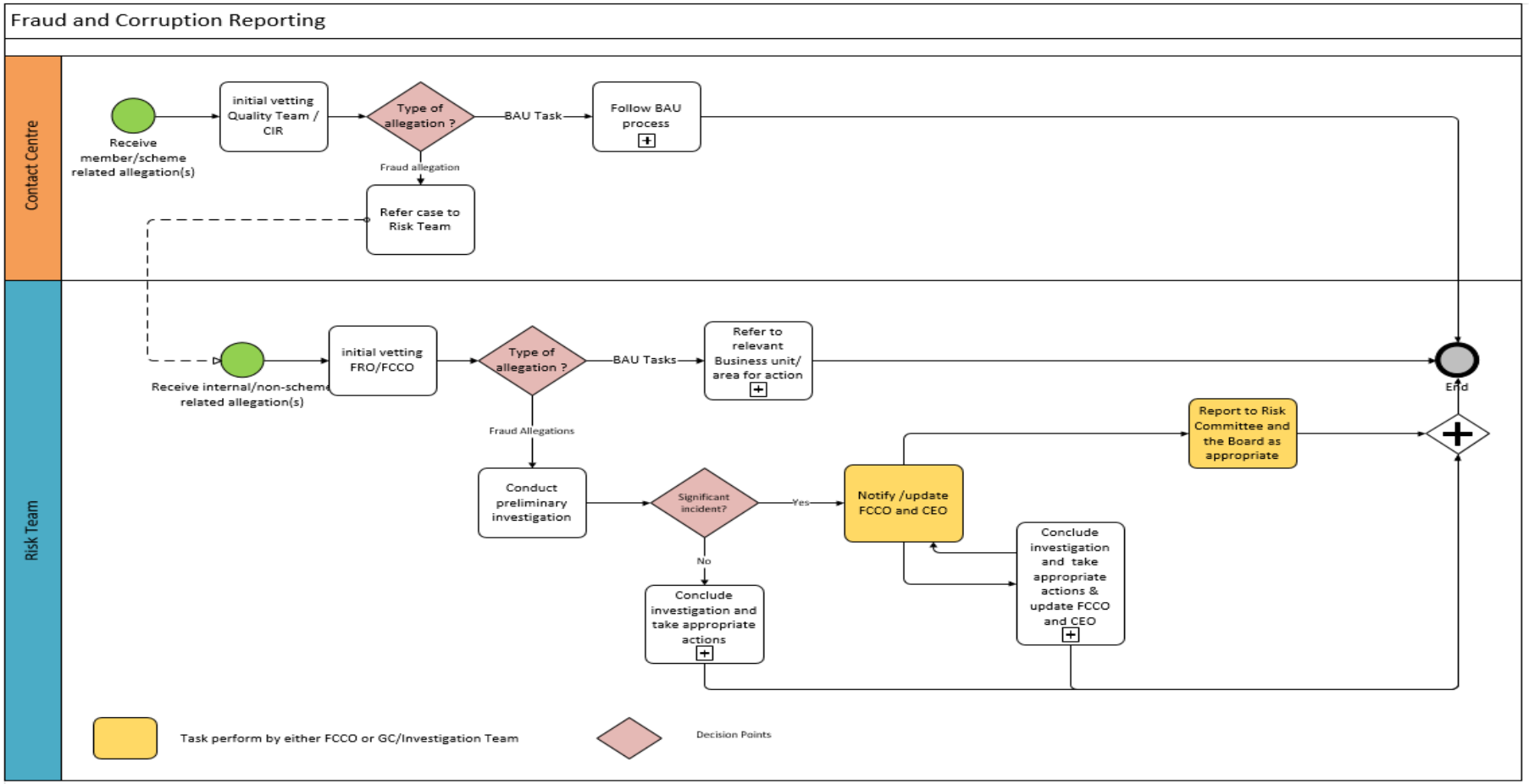
Task	Responsibility	Timing
Undertake fit and proper assessment as CSC per the Fit and Proper Policy	General Counsel	Ongoing
Reporting gifts, entertainment or other relevant interests in the Gifts and Conflicts Register.	Employees	As required
Conducting third party due diligence on suppliers.	Executive[4] Managers/relevant business areas	As required
Identifying potential risks of fraud, scams and corruption in systems and processes in their area and reporting all suspicions of fraud and corruption.	Employees	Ongoing
Identifying potential risks of fraud, scams and corruption in systems and processes under their control and implementing systems and controls to prevent and detect instances of fraud and corruption.	Executive and FCCO	Ongoing
Provide the opportunity for departing employees to disclose any suspicions of fraudulent or corrupt activity at exit interview.	Executive Manager, People	Ongoing
Providing advice of fraud, scam and corruption risk and internal control issues.	Fraud Risk Analyst and FCCO	Ongoing
Establishing centralised referral points for allegations of incidents of fraud, scam and corruption, inclusive of ensuring all matters are appropriately recorded, investigated, referred (where and when appropriate) and reported.	Fraud Risk Analyst and FCCO	As required
Appointing an external investigator (if required).	FCCO	As required
Assisting in the use of administrative remedies.	General Counsel	As required

[4] For the purposes of this Plan, Executive Mangers include all Executive Managers, Chief Operations Officer, Chief Investments Officer and Chief Customer Officer.

Task	Responsibility	Timing
Referring a public interest disclosure to the NACC regarding a CSC employee (current or former) which the investigating officer suspects may involve serious or systemic corrupt conduct (NACC Act s35).	Officer investigating	As required
Referring a corruption issue to the NACC regarding a CSC employee (current or former) which the CEO suspects may involve serious or systemic corrupt conduct (NACC Act s33).	Chief Executive Officer	As required
Reporting a fraud or scam incident to the Police and other external parties.	FCCO	As required
Reporting a fraud or scam incident to the regulators (e.g. APRA and/or ASIC).	General Counsel	As required
Managing media interest in any fraud, scam or corruption incident (in accordance with CSC's Media Management Policy).	Corporate Affairs Manager	As required
Pursuing the recovery of losses associated with fraud and corruption.	Customer Operations on advice from General Counsel	As required
Notifying the insurers of a fraud, scam or corruption incident.	General Counsel	As required
Co-ordinating a review of CSC internal controls following a fraud, scam or corruption incident.	FCCO and relevant Executive Manager	As required
Recording all fraud allegations and directing for investigation to the appropriate business area for action (if referral is BAU in nature).	Contact Centre - (member or scheme related allegations) Fraud Risk Officer/FCCO (Internal or non-scheme related allegations)	Ongoing
Undertaking investigations of allegations of fraud and taking appropriate actions: Responsibility for maintaining an appropriate recording and tracking Plan to facilitate satisfactory resolution of instances of suspected fraud and corruption referred to team	Fraud Risk Officer	Ongoing

Task	Responsibility	Timing
Providing an aggregated report to the Risk Committee summarising the fraud, scam and corruption incidents and actions taken.	FCCO	Annual
Per s33(a)(ii) of the FAR Act, 'scam management' is a key function that has been allocated to the Customer Group Executive and Chief Risk Officer.	Customer Group Executive and CRO	Ongoing

Appendix B – Reporting framework



Appendix C - Contact details

Fraud reporting (Internal / Non-Scheme related):

Email: fraud.control@csc.gov.au

Fraud reporting (Member / Scheme related):

Phone: Call Centre Contact numbers as provided by Scheme Web Page

Email: fraud.report@csc.gov.au