Fraud and Corruption Control implementation guide

Guidance for portfolio entities

This guide supports governance and integrity staff at portfolio entities to implement the Australian Standard for Fraud and Corruption Control.

About this guide

This guide has been developed to support the implementation requirements to align with the Australian Standard for Fraud and Corruption Control (FCC) (the Standard) at the department's portfolio entities. Governance and integrity staff at portfolio entities may refer to this guide to assist in revising their policies and procedures to reflect the Standard.

The guide is comprised of four parts:

Part 1: Introduction

This introductory section provides an overview of the Standard, including its scope and applicability to portfolio entities. This section also outlines key changes to the Standard in 2021.

Part 2: Implementation guide

The implementation guide contains a step-by-step process to update policies and procedures in accordance with the Standard. This includes a policy review, consultation with stakeholders and the development of key documents, including the Fraud and Corruption Control Framework/System (Framework) and Plan.

Part 3: Fraud and Corruption Control checklist

The checklist highlights key areas of compliance to be demonstrated in the Framework. The checklist also notes co-requisite Standards and highlights areas of overlap with existing compliance requirements for public entities within the Victorian Public Sector.

Part 4: External resources

This section contains a list of external resources with further guidance on Fraud and Corruption Control, including guidelines from the Commonwealth Fraud Prevention Centre, the Victorian Public Sector Commission (VPSC) and the Independent Broad-based Anti-corruption Commission (IBAC).

It is recommended that this guide be read in conjunction with the FCC model policy and series of FCC factsheets.

If you have any questions regarding the implementation of Fraud and Corruption Control at your public entity, please contact governance@delwp.vic.gov.au or integrity@delwp.vic.gov.au for advice.

delwp.vic.gov.au

VICTORIA State Government | Environment, Land, Water and Planning

Part 1: Introduction

About the Standard

The Australian Standard for Fraud and Corruption Control (AS8001: 2021) (the Standard) is considered the industry benchmark for mitigating fraud and corruption control (FCC) risks in organisations. The Standard provides guidance and recommendations to mitigate FCC risks across a broad range of business functions, including integrity, governance, finance, cybersecurity and risk. The Standard adopts a holistic approach to managing FCC risks and emphasises a shared responsibility to address fraud and corruption within organisations.

All Australian organisations are expected to comply to the Standard, or to demonstrate plans to achieve compliance over a longer span of time. Some smaller entities with fewer resources may find it challenging to achieve full compliance with the Standard, due to its broad and comprehensive range of mitigation actions. Any outstanding areas may be incorporated into a Fraud and Corruption Control Plan (Plan) to inform business planning and longer-term implementation efforts.

Structure and approach

The Standard consists of five sections:

1. **Scope and approach** sets out the Standard's scope and applicability, and includes definitions as well as co-requisite Standards (see Implementation checklist for further information).

2. **Foundations for fraud and corruption control** describes the broad actions to be undertaken in mitigating FCC risks. These include setting out the roles and responsibilities of all involved in managing FCC risks. This includes the role of the governing body (board) and senior management in acknowledging FCC as a serious risk and demonstrating a high level of commitment to mitigation efforts.

   This section also introduces the FCC System or Framework (the Framework) as a comprehensive framework that incorporates the organisation's prevention, detection and response initiatives, across a broad range of responsible business functions.

3. **Preventing fraud and corruption** outlines requirements and recommended initiatives to proactively prevent fraud and corruption incidents from occurring in organisations. These include the promotion of an integrity framework, policies and procedures relating to conflicts of interest and gifts, benefits and hospitality, and preventing technology-enabled fraud.

4. **Detecting fraud and corruption** provides a series of initiatives for organisations to implement in the proactive detection of fraud and corruption. These include financial management, data analytics and reporting, human resources, and ensuring clear reporting channels and protections for disclosers.

5. **Responding to fraud and corruption events** includes a series of required procedures and recommended actions to take in response to fraud and corruption incidents. These range from immediate actions to take on discovery of a fraud and corruption incident through to longer-term response and recovery plans.

Revisions to the Standard in 2021

The Standard was revised in 2021, in its first update since 2008. The revised Standard has brought the document up-to-date to reflect the increasing role of integrated technology in business management and associated expectations for effective fraud and corruption control. Some key changes to the Standard include:

• 'Fraud control plans' are now referred to as 'Fraud and Corruption Control Systems' (or Frameworks)

• Updated definitions for fraud and corruption, as reflected in the FCC model policy

• New requirements for organisations to consider external threats, particularly cyber-security risks, in their prevention, detection and response plans

- The introduction of 'normative references', or co-requisite Standards, which must be complied with to achieve full compliance with the FCC Standard

- Greater emphasis on the role of boards and senior management in setting the tone from the top and demonstrating a serious commitment to addressing fraud and corruption risks

- Requirement to implement a 'pressure-testing' system to evaluate the effectiveness of control measures across a range of high-risk business areas including finance and information technology

- Immediate actions to be taken in response to fraud and corruption incidents, including the capture of digital evidence, to ensure that these incidents may be investigated and addressed as needed.

Areas covered by existing Victorian Public Sector requirements

Many of the Standard's requirements represent existing obligations for entities within the Victorian Public Sector. These include processes for financial management, management of conflicts of interest and gifts, benefits and hospitality, public interest disclosures, cybersecurity and risk management.

It is recommended that organisations refer to the Victorian Government requirements listed below as a minimum starting-point to address these areas:

- Code of Conduct for Victorian Public Sector Employees

- Code of Conduct for Directors of Victorian Public Entities

- IBAC guidance on public interest disclosures

- Standing Directions 2018 under the Financial Management Act 1994

- Victorian Government Cyber security standard and guidelines

- Victorian Government Risk Management Framework

- VPSC conflict of interest guidance for organisations

- VPSC gifts, benefits and hospitality resource suite

- VPSC guide to pre-employment misconduct screening

Part 2: Implementation guide

Introduction

This section introduces a recommended step-by-step process for governance and integrity staff to assist in the implementation of the Standard. While this section describes a recommended process for larger organisations, the process may vary depending on resourcing and risk appetite.

Step 1: Review

Review your organisation's current FCC System/Framework/Plan against implementation checklist and the Standard, noting any areas to be added or updated for compliance. These may range from updated definitions in your organisation's FCC policy to longer-term initiatives and prevention mechanisms.

Step 2: Consult

Consult with the relevant business units that are responsible for each area of Fraud and Corruption Control. These may include Financial compliance, Grants, Procurements, Information Technology, Human Resources, Asset Management and Risk. These consultations provide an opportunity to clarify the shared responsibility in managing fraud and corruption risks, and to confirm that the relevant practices required under the Standard are in place or can be implemented.

Step 3: Draft FCC System/Framework

Draft a revised FCC System or Framework to reflect your organisation's holistic approach to fraud and corruption control. This document should reflect the procedures set out in the Standard and the implementation checklist. Any areas which require further implementation may be noted in the document and included in your organisation's Plan. Confirm content for each relevant business area with relevant stakeholder (ie. procedures relating to post-transactional review or financial management may be drafted or reviewed by Finance staff).

Step 4: Prepare a fraud and corruption control policy

Prepare a FCC policy to set out your organisation's position on fraud and corruption control. The policy should include updated definitions and a commitment to taking fraud and corruption seriously. The FCC model policy may be adapted as needed to reflect your organisation's stance.

Step 5: Compile a fraud and corruption control plan

The Plan should include any areas that haven't achieved full compliance with the Standard and which may require implementation over a longer period of time. For example the organisation may commit to implementing a pressure-testing program or environmental scan within the next calendar year.

Step 6: Develop a communications strategy

Develop a communications strategy to raise awareness of fraud and corruption control and relevant staff obligations. The strategy should also consider measures to foster an organisation of integrity with a safe Speak Up! culture that enables staff to recognise and report any cases of suspected misconduct or corruption. The FCC factsheets provide further information and key messages that can be tailored for your communications.

Step 7: Finalise and distribute key FCC documents

Once an appropriate level of sign off has been reached, you may wish to publish and distribute your FCC Framework, Plan and Policy to staff. Further actions can be taken to implement your communications strategy and address any areas of non-compliance over a longer time horizon.

Part 3: FCC framework/system checklist

Introduction

This section provides a checklist of recommended areas to address in your organisation's FCC Framework or System (Framework). Please note that this list is non-exhaustive and is designed to complement the Standard. For further information please refer to the Standard, which contains guidance and detailed advice on each area.

Structing the Framework

The FCC Framework provides a high-level overview of the mechanisms in place to prevent, detect and respond to fraud and corruption incidents, demonstrating compliance with the Standard. This figure outlines the recommended structure of the Framework:

Prevent – Proactive elements to prevent fraud and corruption

Detect – Actions to increase the likelihood of detecting fraud and corruption

Respond – Actions to respond to detected fraud and corruption incidents

Foundations of fraud and corruption control: planning and resourcing

Checklist of items to be included in an FCC Framework or System:

Section 1 - General
☐ Include a clear statement of your organisation's tolerance levels for i) fraud and corruption incidents (zero) and ii) risk of fraud and corruption incidents (low)
☐ Demonstrate organisation's commitment to upholding the Victorian Codes of Conduct for Public Sector Employees and Directors
☐ Describe how the FCCF links to other policies, plans and guidelines or frameworks as part of a holistic approach to managing fraud and corruption

Section 2 - Foundations
☐ Set out key roles and accountabilities for the board, executives, senior management, specialist functions and line managers – ie. ensuring a collective responsibility to managing FCC incidents, and communicating accountability for fraud to applicable business units
☐ Include activities that contribute to an ethical culture, including education and training, communications and adequate controls and policies
☐ Describe risk management procedures for the management of any identified fraud and corruption risks

☐ Commit to undertaking an environmental scan at least biennially or during significant changes such as an organisational restructure *(refer to PESTLE guidance in FCC factsheets)*

☐ Outline priority areas in an FCC Strategy or Plan – identify risk mitigation activities across the organisation that require implementation or improvement over a longer time horizon

☐ State the organisation's commitment to implementing or maintaining an internal audit program that will include the identification of fraud and corruption risks

☐ Acknowledge external threats and controls, for example by implementing a cyber security program and information security management system

☐ List the policies, procedures and systems in place where employees maintain accurate and complete records of business activity and maintain confidentiality requirements

Section 3 - Prevent

☐ Develop and implement a communications plan to raise awareness of the organisation's approach to managing risks of fraud and corruption, including relevant policies, frameworks and obligations for staff under the Code of Conduct.

☐ Set out relevant financial management and procurement policies, procedures and controls such as accounts reconciliation

☐ Design, implement and promote an integrity framework in accordance with the structure recommended under section 3.2 of the Standard. (Note that the department will provide further support in this space in early 2022)

☐ Describe recruitment procedures and pre-employment screening internal controls *(see VPSC guidance)*

☐ Outline the range of internal controls that are in place to prevent fraud in procedures, such as segregation of duties

☐ Describe processes for Gifts, Benefits, Hospitality and donations management and maintenance of register

☐ Describe processes for Conflict of Interest management and maintenance of a declarations register

☐ Implement a 'pressure testing' program to test internal controls *(further information can be found in section 3.5.3 of the Standard and in the External Resources section at the end of this factsheet)*

☐ Outline personnel security measures such as physical access controls and identification procedures

☐ Outline asset management measures to prevent theft or loss

Section 4 - Detect

☐ Implement and set out the organisation's approach to data analytics, ie. providing regular reports to senior leaders outlining patterns and trends in fraud and corruption threats, incidents and investigations

☐ Confirm any financial post transactional measures in place such as corporate card account reviews and analysis of accounting reports

☐ Understand and identify early warning signs (see FCC early warning signs factsheet)

☐ Describe Public Interest Disclosure policy which outlines reporting options and channels

☐ Describe the exit interview process for terminated staff as a way of identifying FCC incidents

Section 5 – Respond
☐   Develop and describe a procedure for immediate action in response to a fraud and corruption event
☐   Describe organisation's procedures to ensure complaints are directed to the correct person at the organisation or the appropriate agency (such as IBAC)
☐   Confirm that the organisation is insured against fraud and cyber security (appropriate for the size and risks of the organisation)
☐   State the organisation's approach to implementing recommendations from audits and reports.

Compliance with other Standards

Standards Australia now requires compliance with further Australian and International Standards in order to achieve full compliance with the FCC Standard. The full list of prerequisite Standards includes:

- AS4811, *Employment screening*
- AS ISO 31000, *Risk management – Guidelines*
- AS ISO 37001, Anti-bribery management systems
- AS ISO/IEC 27001, Information technology – Security techniques
- ISO/IEC 27037, Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence
- ISO/IEC 27041, Information technology – Guidance on assuring suitability and adequacy of event investigative method
- ISO/IEC 27042, Information technology – Guidelines for the analysis and interpretation of digital evidence
- ISO/IEC 27043, Information technology – Incident investigation principles and processes
- ASA 240 The Auditor's Responsibility Relating to Fraud in An Audit of a Financial Report issued by the Auditing And Assurance Standards Board
- NIST SP 800-61 Revision 2, Computer Security Incident Handling Guide.

Governance and integrity staff are encouraged to consult with internal stakeholders such as Finance and Information Technology to confirm compliance with the above Standards, noting that most are already covered by existing Victorian Government requirements.

Part 4: External resources

Fraud and Corruption Control

Australian Institute of Company Directors Insights

BDO Australia: Fraud and corruption control checklist for Boards and Executives

Commonwealth Fraud Prevention Centre: Guidance on pressure testing

IBAC - Controlling fraud and corruption: a prevention checklist

Victorian Managed Insurance Authority – PESTLE factsheet

Victorian Public Sector Commission – Understand your environment factsheet

Victorian Government policies and frameworks

Code of Conduct for Victorian Public Sector Employees

Code of Conduct for Directors of Victorian Public Entities

IBAC guidance on public interest disclosures

Standing Directions 2018 under the Financial Management Act 1994

Victorian Government Cyber security standard and guidelines

Victorian Government Risk Management Framework

VPSC conflict of interest guidance for organisations

VPSC gifts, benefits and hospitality resource suite

VPSC guide to pre-employment misconduct screening

For more information please also refer to the FCC factsheets and model policy.

Accessibility

If you would like to receive this publication in an alternative format, please telephone the DELWP Customer Service Centre on 136186, email customer.service@delwp.vic.gov.au, or via the National Relay Service on 133 677 www.relayservice.com.au. This document is also available on the internet at www.delwp.vic.gov.au.