Australian Standard on Fraud and Corruption Control (AS 8001:2021)

Overview

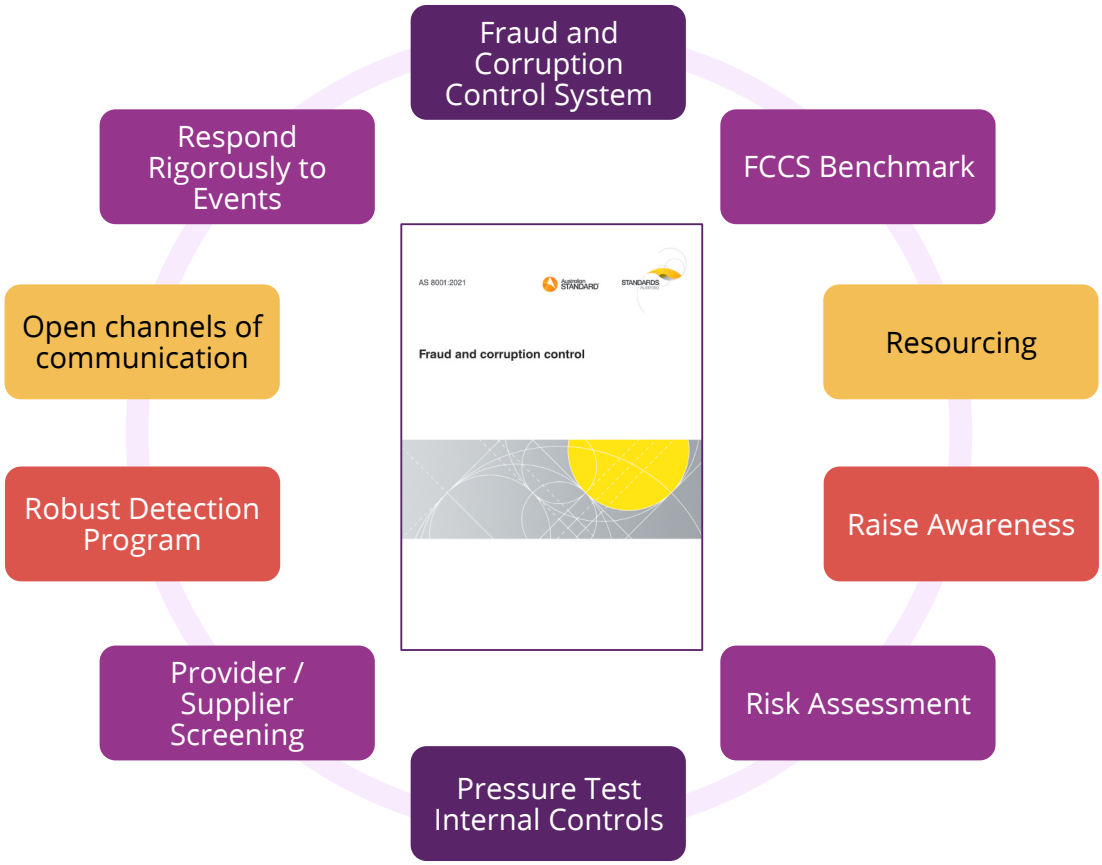
The *Australian Standard on Fraud and Corruption Control* (AS 8001:2021) is a useful framework for assisting Victorian public sector agencies, local government and Victoria Police to control their fraud and corruption risks across all aspects of their operational and administrative functions. The Standard provides guidance on the minimum requirements recommended to develop, implement and maintain an effective fraud and corruption control system to enhance:

- Prevention
- Early detection
- Effective response.

You can purchase a copy of the *Australian Standard on Fraud and Corruption Control* (AS 8001:2021) at the Australian Standards store.

Top 10 anti-fraud and corruption initiatives

IBAC has identified 10 anti-fraud and corruption initiatives that organisations can apply based on the guidance provided in the Standard to prevent fraud and corruption.



This summary is designed to complement the Standard. For guidance and detailed advice on each area, refer to the Standard.

Fraud and Corruption Control System

1. Implement and maintain a fraud and corruption control system (FCCS)

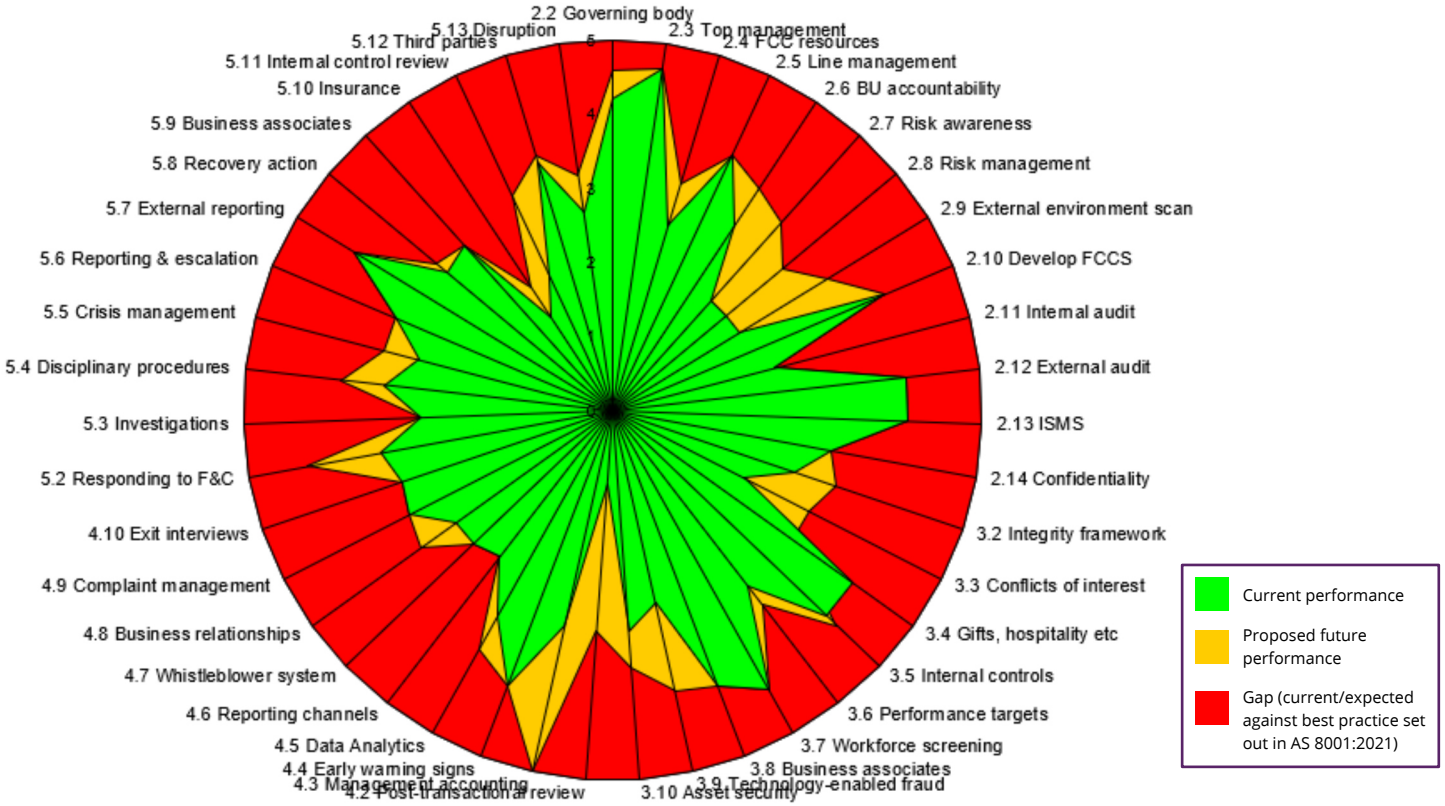
Corruption prevention principles form an integral part of corporate, strategic and operational planning processes and objectives, both annually and long term. An organisation should ensure it has a fraud and corruption control system in place and a program for monitoring and updating it periodically. This should be designed based on the framework set out in the Standard.

FCCS Benchmark

2. Compare your organisation's FCCS against the Standard

Identify gaps between the current and desired future state to help prioritise actions. One way to do this is to assess the organisation's current performance against each section of the Standard and compare this against the desired future state for the organisation on those same elements.

An option to display this is to use Microsoft Excel and produce a spider-web chart. This can be an effective way to present the information to senior management, boards and Audit and Risk Committees.



Arrangements should be in place that ensure effective ongoing scrutiny of the effectiveness of the system to consider whether it continues to meet the organisation's needs. This should be overseen by executive management, internal audit and audit committees

Each organisation will have specific but differing levels of risk across the organisation and its services. In determining the best approach to managing these risks, the resources used for preventative strategies should be proportionate to the organisational risk profile.

Refer to section 2.10 AS 8001:2021 for more information.

Resourcing

3. Make sure adequate specialist resourcing is in place

Inadequate fraud and corruption control resourcing is a major shortcoming in many organisations across all sectors. Consider if the organisation has adequate specialist resourcing (part-time/full-time) and, if not, should appoint adequately qualified and experienced staff or external providers. Consider areas identified as at risk, such as procurement, finance, HR, compliance and risk management, and information security.

Promote collaboration between all fraud and corruption control specialist resources. Consider having a member of the executive management as the central point of contact for fraud control policies within the organisation.

Refer to section 2.4 AS 8001:2021 for more information.

Raise Awareness

4. Develop and implement a program for raising awareness across the organisation

Ensure people in high-risk positions, such as procurement, revenue receipt, or who have discretionary decision-making roles are appropriately trained, supervised and supported. This should also include awareness raising for those in governance and senior executive levels.

Upskill supervisors so they're alert to signs of stress experienced by staff or of other unexplained changes in behaviour or attitude, particularly holders of high-risk roles. Awareness raising and training should also be considered for volunteers, contractors and suppliers.

Build messaging into induction programs periodically throughout the year (appropriate to the organisation's risks) and on significant changes in processes or risk exposures.

To assist with raising awareness, explore global and local trends, industry-specific exposures, organisational incidents in recent years and specific organisational risks. Develop clear statements of expectation regarding staff and zero tolerance regarding fraud and corruption.

Refer to section 2.7 AS 8001:2021 for more information.

Risk Assessment

5. Implement a rigorous program of fraud and corruption risk a assessment

Apply the AS ISO 31000:2018 Risk management Guideline to assess the likelihood and consequence of each risk to determine the 'risk level' (eg low – very high).

In identifying fraud risks, consider the organisation's size and function, any change in structure or function, external and internal fraud risks, new and emerging fraud risks, and the broader organisational operating environment risks to develop a fraud and corruption risk profile.

Refer to section 2.8 AS 8001:2021 for more information.

Pressure Test Internal Controls

6. Implement a 'pressure testing' program

The scale and form of pressure testing should align with an organisation's risk profile. This involves introducing documents, data or other actions consistent with an actual fraud or corruption event to determine if existing internal controls are operating as intended.

Examples of fraud that could be the subject of pressure testing include:

- Credit card misuse (eg purchase for personal use by a senior executive)
- Internally generated false invoices by a member of the Accounts Payable team (work not ordered, not delivered)
- Grant funding fraud (eg improper approval of a fraudulent application for grant funding by a community group)
- Payroll manipulation (eg changes to payroll masterfile to redirect an employee's salary to another bank account without their knowledge).

Refer to section 3.5 AS 8001:2021 for more information.

Provider / Supplier Screening

7. Implement a program aimed at assuring the integrity of employees, providers and suppliers

For employees, ensure there is an established pre-employment screening policy, including employment, qualifications, credit, criminal history and reference checks, which can help identify potential issues and factors that may be indicative of fraud risk, such as prior criminal convictions for dishonesty.

For providers and suppliers, consider the organisation's due diligence processes in place to verify business associates (suppliers, providers, customers, clients) and any risks associated with them; consider requiring business associates with a high risk of fraud to implement their own fraud and corruption control system; look at the contractual terms in place between the organisation and business associate.

Refer to section 3.8 AS 8001:2021 for more information.

Robust Detection Program 8. Consider controls that 'disrupt' the plans of perpetrators

Since it's not always possible to successfully investigate fraud and corruption, organisations should consider controls that 'disrupt' the plans of perpetrators.

Fraud/corruption event	Disruption control
Supplier bank account numbers have been fraudulently changed resulting in invoice payments being stolen by a crime gang.	All email or phone requests to change bank accounts are confirmed by a phone call to the supplier until an alternate system is developed.
Losses have been suffered following online sales made to customers using stolen credit card details.	An online sales channel is closed until a method of detecting stolen credit cards details is developed.
Customers of a superannuation fund have had their login details stolen and funds fraudulently withdrawn from their accounts.	Withdrawal of funds directed to recently changed bank accounts are stopped until the transaction is confirmed as legitimate by contacting the member.
Confidential information relating to the awarding of contracts is repeatedly leaked in an anonymous online portal everytime a new contract is awarded.	Access to the contracts database (edit and view) is closed until access controls are reviewed and amended.

Refer to section 4 AS 8001:2021 for more information.

Open channels of communication 9. Make sure open channels of communication are available

The most common way fraud and corruption is detected is through workplace observation. That's why it's important to ensure open channels of communication are available to encourage the workforce to come forward to report suspected unethical behaviour such as fraud or corruption (eg reporting to line management, internal audit or via a hotline). A range of internal and external reporting mechanisms should be available and accessible to employees, suppliers and the broader community. Anonymity must be permitted.

Establish mechanisms, policies and procedures for supporting and protecting disclosers as required by the *Public Interest Disclosures Act 2012 (Vic)*. Maintain strict confidentiality from the outset in the receipt and processing of reports of fraud and corruption.

Refer to section 4.6 AS 8001:2021 for more information.

Respond Rigorously to Events

10. Implement a zero-tolerance fraud and corruption policy

Implement a zero-tolerance fraud and corruption policy. Follow through on the policy when incidents are detected by taking appropriate action. For example, investigate in accordance with the organisation's policy, and where appropriate, suspend workers and/or take civil or criminal action.

Refer to section 5 AS 8001:2021 for more information.