audit office
OF NEW SOUTH WALES

Fraud Control Improvement Kit

February 2015

Managing your fraud control obligations

From the Auditor-General

I encourage organisations to implement a sound fraud control framework

Fraud control requires an ongoing commitment that goes well beyond setting up policies and procedures.

This revised Audit Office's Fraud Control Improvement Kit recognises the importance of the cultural elements of fraud control and how leaders in an organisation can play a role in ensuring the right culture is present. The approach to fraud control should be positive and proactive and fraud control should not be a 'tick and flick' exercise.

The Improvement Kit is designed to help organisations meet the challenge of implementing an effective fraud control framework. It provides guidance on the key elements of the framework and contains practical resources to help organisations implement, review and monitor the framework.

I encourage organisations to implement a sound fraud control framework which is specific to their internal and external operating environment and is proportionate to the fraud risks.

Grant Hehir
Auditor-General

February 2015

Acknowledgments

This Fraud Control Improvement Kit builds on previously issued Audit Office publications and we acknowledge the contributions made to these resources. In particular we would like to thank those individuals and agency representatives who contributed to the development of the Fraud Control Improvement Kit 2006.

We would also like to thank those representatives from NSW Government agencies who provided valuable feedback on the development of this latest Fraud Control Improvement Kit.

Contents

Executive Summary

Helping organisations manage their fraud control obligations

The Audit Office of New South Wales' Fraud Control Improvement Kit provides guidance and practical advice to help organisations implement an effective fraud control framework.

This improvement kit highlights what should be present within an organisation to make fraud control work and aligns with the Standards Australia Fraud and Corruption Control Standard AS8001-2008. Organisations are encouraged to follow this standard in the design and implementation of their fraud control framework.

Why revisit fraud?

The last Audit Office guidance on fraud was the 2006 Better Practice Guide 'Fraud Control Improvement Kit: Meeting Your Fraud Control Obligations', which built on its original fraud control guidance published in 1994.

This updated Fraud Control Improvement Kit consolidates the previously issued resources into one document and places additional focus on the cultural elements that should be present to implement an effective fraud control framework. This responds to feedback from organisations that have used the Audit Office's fraud control guidance and issues identified in the Audit Office's 2012 fraud control survey – published in Auditor-General's Report to Parliament 2012, Financial Audit, Volume Seven focusing on Law, Order and Emergency Services. The 2012 survey identified:

- fraud control was seen as a 'tick and flick' exercise by some agencies
- there was a lack of risk assessment when agencies changed their role or function
- there was growing fraud in outsourced functions
- procurement was the highest risk area for fraud.

Who is responsible for managing fraud?

The fraud control framework is a tool to help organisations discharge their responsibility for preventing, detecting and properly responding to fraud. Each organisation should develop a strategy for implementing this framework which is specific to its own internal and external operating environment and which is proportionate to the fraud risks it faces.

Auditing Standard ASA 240 provides:

> The primary responsibility for the prevention and detection of fraud rests with both those charged with governance of the entity and management. It is important that management, with the oversight of those charged with governance, place a strong emphasis on fraud prevention, which may reduce opportunities for fraud to take place, and fraud deterrence, which could persuade individuals not to commit fraud because of the likelihood of detection and punishment. This involves a commitment to creating a culture of honesty and ethical behaviour.

What's in the Fraud Control / Improvement Kit?

The Fraud Control Improvement Kit sets out the Audit Office's fraud control framework and contains a series of practical resources to help organisations implement that framework.

The fraud control framework

The fraud control framework has ten key attributes, which sit within the themes of prevention, detection and response. Each attribute has a checklist of high-level processes and behaviours that should be present and information on what you might expect to see in a successful fraud control framework.

A commitment to managing fraud should be embedded in the organisation's culture and be integrated within the core business of the organisation. Two of the new attributes,' Leadership' and 'Ethical framework', emphasise the importance of culture in an effective fraud control framework.

The fraud control resources

The appendix contains resources which can be used by organisations to monitor and improve their fraud control framework:

Resource one: Fraud Control Checklist - designed for organisations to quickly assess the adequacy of their fraud control framework.

Resource two: Risk Assessment - guidance on how to assess fraud risk including a sample fraud risk register with examples of typical fraud risks.

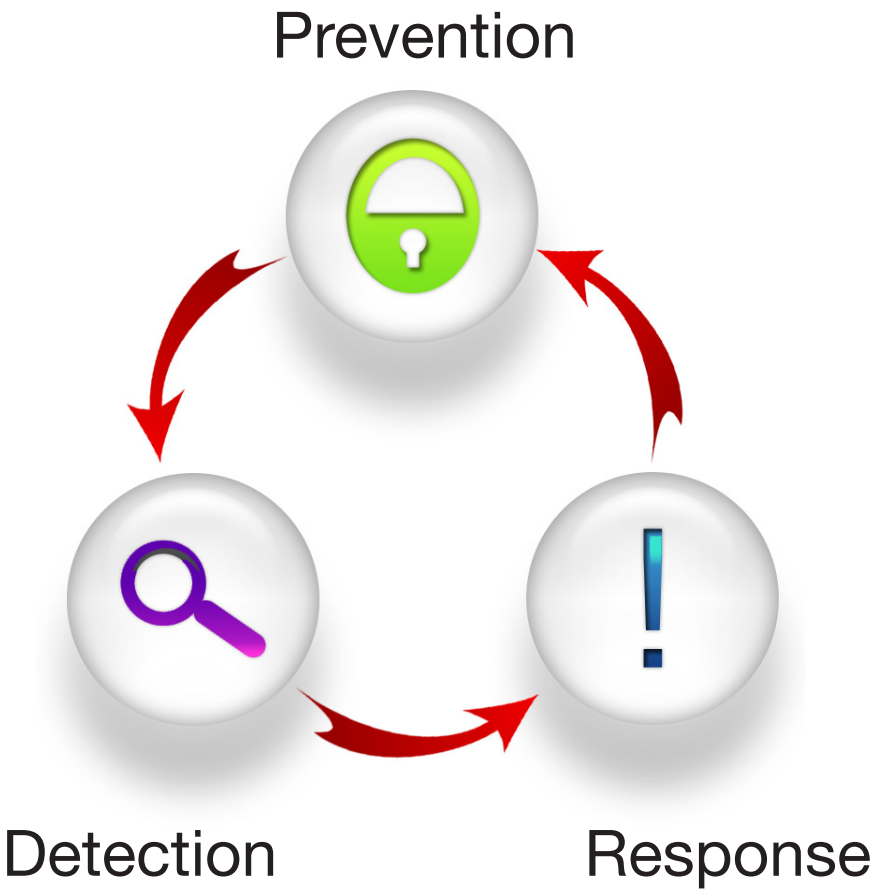
Resource three: Fraud Control Health Check - helps organisations gain a high-level understanding of the extent of employee awareness of fraud control.

Resource four: Fraud Control Improvement Workshops – designed for organisations to follow up in detail on issues identified in the Fraud Control Health Check.

Resource five: Sample Fraud Control Policy – high level overview of a fraud control policy addressing the ten attributes of fraud control.

Resource six: Procurement Checklist – recognises that procurement is a significant area of fraud risk.

The improvement kit can be used by public and private sector organisations, although references to legislation and directions relate to NSW Government agencies.



The fraud control framework

Atrribute one: Leadership

Checklist

1. CEO and senior management commitment to fraud control:

- ❒ CEO visibly endorses fraud control activities
- ❒ senior managers demonstrate their commitment to mitigate fraud risks.

2. Clearly defined CEO and senior management accountability and responsibility:

- ❒ senior management assigned responsibility for implementing the fraud control framework
- ❒ senior managers' individual performance agreements contain performance measures and indicators relating to successful fraud control.

Resources – Fraud Control Health Check (resource three), Fraud Control Improvement Workshops (resource four).

A successful fraud control framework is led by a committed and accountable executive. The commitment to managing fraud starts at the top. Without effective engagement by senior management, the rest of the organisation is unlikely to be committed.

Talking about setting the right tone at the top of an organisation is easy; identifying what this looks like is much more difficult and may look different for different organisations. However, there are some common elements:

1. CEO and senior management commitment to fraud control

The CEO should be seen to be visibly endorsing the organisation's fraud control activities. This may be helped by regularly presenting on the topic to senior managers, emailing staff, publishing articles on the intranet or by promoting the fraud control framework via a podcast to the whole organisation.

Senior managers should demonstrate their commitment to mitigating the fraud risks facing their organisation for example, championing the risk assessment process and including fraud as a priority item in management meetings. Managers should focus on the areas with the highest inherent fraud risk, such as procurement and payments. It is important for senior managers to demonstrate a positive and proactive attitude to fraud control, for example using internal audit findings as an opportunity to improve processes, rather than as a criticism of current practice.

In the NSW public sector, the *Government Sector Employment Act 2013* (GSE Act) gives Department Secretaries and heads of agencies responsibility for the general conduct and management of their agencies in accordance with the core values of the Ethical Framework for the government sector.

2. Clearly defined CEO and senior management accountability and responsibility

It is essential for staff to have confidence in the integrity of their senior managers and CEO. One way of fostering this confidence is to make senior managers accountable for implementing the fraud control framework.

All senior managers and the CEO should be responsible for fraud control as part of their broader ethical responsibilities, with the specific responsibilities of overseeing and driving fraud control processes being assigned to the appropriate senior managers. This can be done in several ways including allocating responsibility in corporate and management plans to individual senior managers. Where appropriate, individual performance agreements could include the successful implementation of the fraud control framework as a performance outcome and indicator.

The Public Service Commission's (PSC's) capability framework for the NSW public sector includes 'acting with integrity' as a key personal attribute expected by the NSW public service. This capability framework provides the structure to incorporate the management of fraud into individual performance agreements and work plans.

The fraud control framework

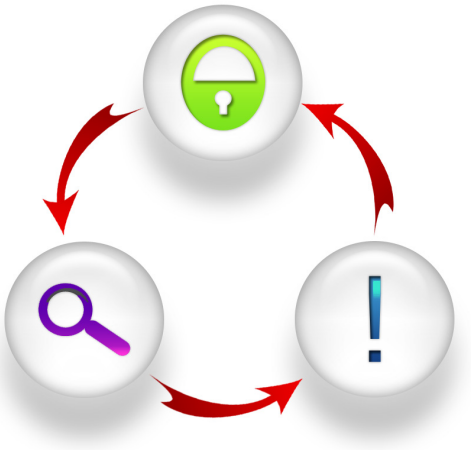
Attribute two: Ethical framework

Checklist

3. Clear policies setting out acceptable standards of ethical behaviour:
- ❒ staff have easy access to all ethical behaviour policies
- ❒ ethical behaviour policies are included in the induction process.

4. Demonstrated compliance with the ethical framework:
- ❒ staff annually evidence their commitment to acceptable standards of behaviour.

5. Employees can articulate obligations to ethical behaviour and the organisation's position on fraud:
- ❒ staff understand fraud is not tolerated and the consequences of committing fraud.



Resources – Fraud Control Health Check (resource three), Fraud Control Improvment Workshops (resource four).

An organisation's fraud control framework is part of a much bigger ethical framework that guides the values of the organisation and provides standards for behaviour and decision-making. The ethical framework sets the organisational culture that is fundamental to the success of a fraud control framework.

In the NSW public sector, the ethical framework is covered in the NSW Public Service Commission's (PSC) 'Behaving Ethically: a guide for NSW Government sector employees' – a package of resources designed to help government sector employees better understand their obligation to act ethically and in the public interest. Public sector agencies should ensure their code of conduct aligns with the PSC Code of Ethics and Conduct. Ethical behaviour policies, such as the code of conduct, should reflect the core values set out in section 7 of the GSE Act 2013.

In the fraud control context, an ethical framework should contain:

3. Clear policies setting out acceptable standards of ethical behaviour

Staff need access to policies setting out acceptable standards of ethical behaviour, including the code of conduct, gifts and benefits policy, conflicts of interest policy and secondary employment policy. Policies should be regularly reviewed and kept up-to-date.

Policies should be readily accessible on the intranet, ideally in one central location. Hard copies should be provided to staff without access to the intranet. Reference to these policies should be included in the new employee induction process.

4. Demonstrated compliance with the ethical framework

Organisations should require staff to annually evidence their commitment to acceptable standards of ethical behaviour. This can be achieved by staff re-signing the code of conduct. However, this should not be a substitute for a wider program of education and awareness – see attribute six.

An important part of the ethical framework is a compliance culture, which recognises organisations have an obligation to comply with legislation and should adopt appropriate standards.

A compliance culture cannot exist in isolation from the rest of the organisation. It should be part of the overall business strategy and operations. Taking an integrated approach to compliance will reduce the perceived burden of compliance and lead to more efficient ways of working.

5. Employees can articulate obligations to ethical behaviour and the organisation's position on fraud

Staff are a key resource in preventing and detecting fraud and it is critical all staff understand their organisation's ethical framework, rules and requirements. Staff need to understand fraud is not tolerated and the consequences of committing fraud.

Organisations can use the Fraud Control Health Check (resource three) to gain a high level understanding of the extent of employee awareness of fraud control. The health check identifies areas of concern which may be followed up using the Fraud Control Improvment Workshops (resource four).

The fraud control framework

Attribute three: Responsibility structures

Checklist

6. Management and all staff have clearly defined responsibilities for managing fraud:

- ❒ staff are aware of the responsibility structure in the organisation
- ❒ responsibilities for fraud control are contained in role descriptions, where appropriate.

7. Fraud management is integrated with core business:

- ❒ managing fraud risks included in business plans.

8. Resources are allocated to managing fraud:

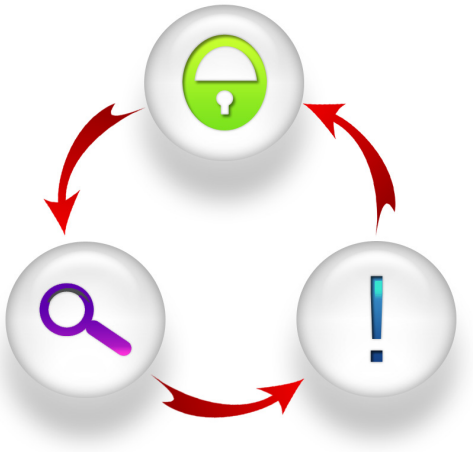
- ❒ fraud committee established and/or a Fraud Prevention Manager appointed.

9. Clearly defined roles for audit and risk committee and auditors:

- ❒ proactive and influential audit and risk committee
- ❒ internal audit work covers controls over high risk fraud areas.

10. Staff with responsibility for fraud control and staff in high risk fraud areas are provided with training:

- ❒ refresher and knowledge update training are provided on an ongoing basis
- ❒ training program is integrated within a wider education and awareness campaign.



Resources – Fraud Control Health Check (resource three), Sample Fraud Control Policy (resource five).

A comprehensive responsibility structure is required to implement an organisation's fraud control framework. Key elements of this structure include:

6. Management and all staff have clearly defined responsibilities for managing fraud

It is important to define responsibility for implementing and monitoring the fraud control framework. Responsibilities at the corporate level need to be clearly set out and those of managers well defined. All staff should be aware of the responsibility structure.

It is important staff recognise everyone in the organisation has a role to play in preventing, detecting and reporting fraud. Organisations are encouraged to use specific examples and relevant case studies as part of an ongoing education and awareness campaign.

At an individual level, it may be appropriate for some role descriptions to include specific fraud control responsibilities. Role descriptions should be revisited and revised after restructures and significant changes in organisational functions. The NSW Public Service Commission's capability framework can be used across a range of management and development activities to embed ethical behaviour as an intrinsic part of each public service role.

7. Fraud management is integrated with core business

An organisation has to accept that managing the risk of fraud is a core part of their business. It is not an 'add on' or separate activity. Managing fraud risks should be included within team and branch plans to demonstrate the process has been integrated. An organisation should use fraud data to inform other business processes. For example, an alleged or actual fraud may highlight weaknesses in a particular system that may also exist in other systems.

A reporting structure should be established to enable operational managers to report fraud risks and mitigating actions taken in response.

8. Resources are allocated to managing fraud

Appropriate resources should be dedicated to fraud control in proportion to the size and risk profile of the organisation. This includes allocating a budget and assigning specific responsibilities.

In larger organisations with significant inherent fraud risks due to the nature and size of its operations, it may be appropriate to establish a fraud control management committee.

This committee should not replace senior management's responsibility for fraud control, but inform and recommend improvements to fraud control frameworks and act as a forum for senior managers to better understand fraud risks and mitigation strategies. Such a committee should include senior officers and staff from a range of areas to provide a balanced approach and help engagement with the business.

It may also be appropriate to appoint a Fraud Prevention Manager; either as a specific appointment, or as part of someone's existing duties. This manager should have delegated responsibility for fraud control within the organisation and act as a central point of contact for all staff.

9. Clearly defined roles for audit and risk committee and auditors

Fraud control roles for the audit and risk committee, internal and external auditor should be clearly defined in accordance with the NSW Treasury 'Internal Audit and Risk Management Policy for the NSW Public Sector (TPP 09-05)' and internal and external auditing standards. It is important that the organisation understands the extent of the responsibilities of these parties.

The audit and risk committee provides independent assurance to the CEO or Board by overseeing and monitoring the adequacy of the fraud control plan and the processes and systems in place to capture and effectively investigate fraud related information. It should review an organisation's fraud control framework at least annually.

Internal audit needs to be alert to the possibility of fraud within an organisation. While management is ultimately responsible for fraud control, internal audit can examine the adequacy of internal controls over high-risk processes and by evaluating the potential for fraud to occur. Internal audit can also undertake specific assignments on the adequacy of the fraud control framework.

10. Staff with responsibility for fraud control and staff in high risk fraud areas are provided with training

Specific training is required for staff primarily engaged in fraud control activities and staff working in high risk fraud areas. Training cannot be a one-off activity. Refresher and knowledge update training should be provided on an ongoing basis. The training program should be integrated within a wider education and awareness campaign, promoting the importance of fraud control (see attribute six).

The fraud control framework

Attribute four: Fraud control policy

Checklist

11. Risk-based policies appropriate to the organisation:

- ❒ appropriate policies address the level and nature of internal and external fraud risks
- ❒ fraud control policy addresses the ten attributes of fraud control.

12. Holistic and integrated:

- ❒ fraud control policy does not operate in isolation and has strong links to other ethical behaviour policies.

13. Regularly reviewed, current and implemented:

- ❒ fraud control policy is responsive to changes in the operating environment and reviewed at least every two years.

Resources – Fraud Control Health Check (resource three), Sample Fraud Control Policy (resource five).

Organisations need to have policies, systems and procedures in place that minimise the risk of fraud throughout the organisation. These should include:

11. Risk-based policies appropriate to the organisation

The nature and extent of the policies, systems and procedures should be appropriate to the level and nature of internal and external fraud risks faced by an organisation. Policies and other documentation should be based on assessed fraud risks. As a minimum, an organisation should have a fraud control policy which addresses the ten attributes of fraud control set out in this framework.

12. Holistic and integrated

The fraud control policy should not operate in isolation. It should have strong links to other ethical behaviour policies, including the:

- PSC's ethical framework for the NSW Government sector
- code of conduct
- statement of business ethics.

A simple way of highlighting the links between the policies is to create an ethical behaviour page on the intranet which brings together all the organisation's policies and procedures around ethical behaviour.

In a successful fraud control framework, all the elements comprising or relating to the fraud control framework will align and not contradict or counter each other.

13. Regularly reviewed, current and implemented

The fraud control policy should be responsive to changes in the operating environment and should be reviewed at least every two years and following significant restructures and/or changes to organisational functions. As already highlighted, it is crucial for the CEO to visibly endorse the policy.

The Fraud Control Health Check (resource three) is a useful way to measure staff understanding of the fraud control policy.

The fraud control framework

Attribute five: Prevention systems

Checklist

14. Proactive and integrated fraud risk assessment:

- ❒ fraud risk assessment is part of organisation's enterprise risk management process
- ❒ risk assessment reviewed after substantial change and at least every two years.

15. Planning, follow up and accountability:

- ❒ fraud control plan in place and outcomes reported to senior managers and audit and risk committee.

16. Analysis of and reporting on suspected and actual frauds:

- ❒ fraud database established containing all reports of fraud, action taken and outcomes
- ❒ database kept up-to-date and published on website.

17. Ethical workforce:

- ❒ pre-employment screening.

18. IT security strategy:

- ❒ specific IT security strategy aligned with the organisation's business strategy
- ❒ cybercrime included as a risk on the risk register.

Resources – Risk Assessment (resource two), Fraud Control Health Check (resource three), Procurement Checklist (resource six).

Fraud prevention systems are a cost effective way to minimise fraud in an organisation. As with all aspects of the fraud control framework, the prevention strategies used by an organisation should be proportionate to the fraud risks involved.

14. Proactive and integrated fraud risk assessment

Fraud risk assessment is key to a successful prevention system and is an important management tool for preventing and detecting fraud. It should be part of an organisation's enterprise risk management process, and cover the organisation's internal and external operating environment.

Extensive material already exists on conducting risk assessments.[1] As a minimum, the fraud risk assessment should identify key functional areas, identify fraud threats within those areas and assess the adequacy of existing controls, both manual and automated controls, to determine any corrective action needed to mitigate fraud risk to an acceptable level. Responsibilities and timeframes for action and reporting should also be included.

A fraud risk assessment should be conducted when there is a substantial change in the function, structure or activities of an organisation and at least every two years. Changes within an organisation such as restructures, contracting out/out sourcing and workforce rationalisation can all contribute to an environment which is susceptible to changing fraud risks. Changes can also lead to out-of-date risk assessments which no longer reflect current operating procedures.

As part of a process of continuous improvement, organisations should monitor the results of the risk assessment over time to help understand the changing risk profile of the organisation. Organisations should also consider benchmarking the results of the risk assessment against those of similar organisations. The results of the fraud risk assessment can be used to inform other business processes and add value to other areas of the business.

15. Planning, follow up and accountability

A fraud control plan should be developed that includes key fraud control activities, responsibilities and timeframes.

The fraud control plan should link to the risk assessment and other fraud control activities, such as the Fraud Control Health Check and the training and education program and contain a summary of the fraud risks, controls and mitigation strategies in place. The fraud control plan should contain information on review mechanisms to enable regular evaluation of the effectiveness of fraud control strategies. It should also assign responsibilities and include timeframes for action.

Ideally, the fraud control plan will be integrated as part of a wider business plan, which will help identify synergies with other areas.

Continues over page

1 Australian National Audit Office Fraud Control in Australian Government Entities, Better Practice Guide March 2011, AS/NZS ISO 31000-2009, AS 8001-2008, Risk Management Toolkit for the NSW Public Sector (TPP12-03).

As with the risk assessment, the fraud control plan should be regularly reviewed and updated (at least every two years) with the outcomes and results of the plan reported to senior management and the audit and risk committee.

16. Analysis of and reporting on suspected and actual frauds

A fraud database should be established containing all reports of fraud, including action taken and outcomes. This database should be regularly reviewed to identify any systemic issues that need attention. The database should be kept up to date and de-identified data published on the organisation's website to demonstrate to staff and the public that fraud is taken seriously and dealt with as part of a transparent and accountable process.

17. Ethical workforce

Each organisation should be committed to employing staff that are suitable for the organisation. It is recommended that a pre-employment screening program be implemented with consideration of Australian Standard AS 4811-2006 – Employment Screening. All new employees and existing employees, who move to key roles within the organisation, should be screened.

As part of the pre-employment screening process, organisations should include standard questions or exercises to help identify whether prospective employees' values align with the organisation's values.

18. IT security strategy

A key element of a prevention system is a specific IT security strategy, which is aligned with the organisation's business strategy. This reflects the significant reliance on technology and the potentially serious consequences of a breach of IT security.

The potential for cybercrime should be included on the risk register and a database kept recording all security incidents. A tested incident response plan should also be in place.

The fraud control framework

Attribute six: Fraud awareness

Checklist

19. Comprehensive staff education and awareness program:

- ❒ ongoing ethical behaviour and fraud education and awareness program
- ❒ fraud control message repeated and reinforced using a variety of communication channels
- ❒ fraud control expectations included in the induction process
- ❒ staff have a good understanding of what fraud is
- ❒ guidance material deals with real life situations, conflicts and fraud risks staff face in their work area.

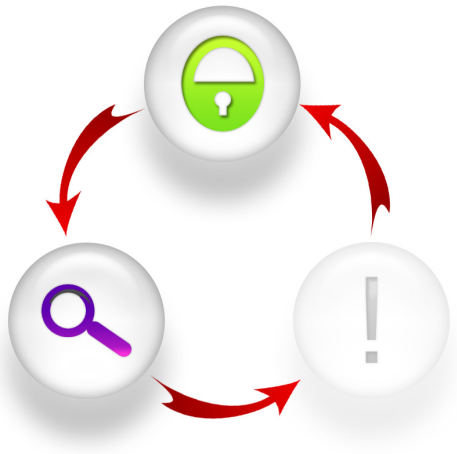
20. Staff awareness of fraud control responsibilities:

- ❒ staff have a good appreciation and understanding of their responsibilities for preventing, detecting and reporting fraud.

21. Customer and community awareness:

- ❒ publicity campaigns developed where appropriate
- ❒ customers and the community encouraged to report suspicions of fraud and provided with easy to use channels to make reports
- ❒ customers and the community have confidence in the integrity of the organisation
- ❒ statement of business ethics setting expectations and mutual obligations.

Resources – Fraud Control Health Check (resource three), Fraud Control Improvement Workshops (resource four), Sample Fraud Control Policy (resource five).



Staff in an organisation are a prime source of information on suspected frauds in their area. To make best use of this valuable resource, staff need to be aware of what fraud is, common types of fraud they may encounter, their responsibilities and how to report suspected frauds. Importantly, the organisational culture has to encourage reporting of suspected frauds (see attribute eight).

A successful fraud awareness program should contain the following elements.

19. Comprehensive staff education and awareness program

An integral element of an effective fraud control framework is an ongoing education and awareness campaign which is regularly reviewed and refreshed.

Training programs in ethical behaviours, including the code of conduct are required. These should be supported by other awareness raising activities, such as newsletters, articles on the intranet and discussion points for team meetings. The fraud control message needs to be repeated and reinforced using a variety of communication channels.

Ethical behaviour policies should be part of the induction process. Guidance material should be specific and deal with the real life situations, conflicts and fraud risks staff may face in their work areas.

It is important staff have a good understanding of what constitutes fraud and that they can articulate the actions needed to address the risk of fraud. Fraud risks will be different for each organisation and the education and awareness program should be tailored accordingly. It should take into account the organisation's size, location, functions and activities.

20. Staff awareness of fraud control responsibilities

All staff need to understand the ethical behaviours expected of them in the workplace. Staff should have a good appreciation and understanding of their responsibilities for preventing, detecting and reporting fraud. This can be demonstrated by requiring staff to re-sign the code of conduct annually, by running specific fraud control improvement workshops (see resource four), or including the topic as a standing item in team meetings.

21. Customer and community awareness

For some organisations it may be appropriate to develop publicity campaigns (where cost effective and appropriate) to highlight fraud risks and the organisation's commitment to manage and mitigate those risks. These campaigns should encourage customers and the community to report circumstances or instances when they suspect fraud is occurring. There should be easy-to-use channels for them to do so, including phone, email and online reporting (see attribute eight).

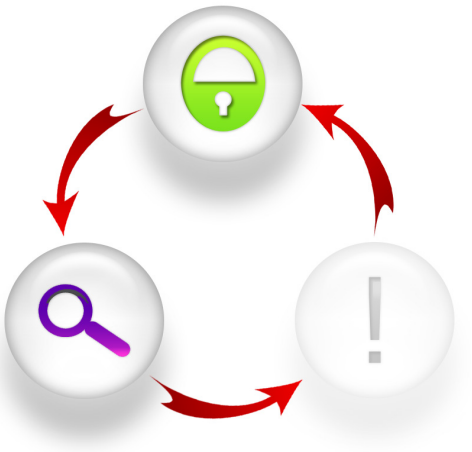
These campaigns help customers and the community have confidence in the integrity of the organisation and understand that it does not tolerate corruption, including fraudulent dealings.

For some organisations, a guarantee of service, customer service charter or statement of business ethics will be sufficient to set out the organisation's position on fraud. Organisations should use the annual report to report on the implementation of the fraud control framework.

The fraud control framework

Attribute seven: Third party management systems

Checklist



22. Targeted training and education for key staff:

- ❒ targeted training and education programs for staff with responsibilities for dealing with third parties.

23. Third party due diligence and clear contractual obligations and accountabilities:

- ❒ structured risk-based due diligence before engaging contractors or third parties
- ❒ contracts and service level agreements include clear accountabilities for managing the risk of fraud
- ❒ position descriptions for staff with responsibilities for managing third parties include accountabilities for managing fraud risks.

24. Effective third party internal controls:

- ❒ specific internal controls relating to third parties in place
- ❒ checks and reviews carried out on dealings with third parties.

25. Third party awareness and reporting:

- ❒ contractors and suppliers understand organisation will not tolerate corruption, including fraudulent dealings
- ❒ statement of business ethics setting expectations and mutual obligations
- ❒ reporting mechanisms established for reporting suspected fraud
- ❒ contractors and suppliers encouraged to provide information if they suspect fraud is occuring.

26. Staff disclosure of conflicts of interest and secondary employment:

- ❒ staff regularly required to disclosure conflicts of interest and secondary employment
- ❒ records of conflicts of interest and secondary employment reviewed and kept up-to-date.

Resources – Risk Assessment (resource two), Fraud Control Health Check (resource three).

Increasingly services are being delivered by third parties which adds an additional layer of complexity to fraud control. Identifying who is responsible for managing fraud is key, as is raising awareness of fraud committed by and against third parties.

22. Targeted training and education for key staff

A specific training and education program should be implemented for staff with responsibility for procurement, contract management and those with other responsibilities for managing third parties. These staff need to be aware of the fraud risks and complexities when services are out sourced or delivered by third parties.

23. Third party due diligence and clear contractual obligations and accountabilities

Organisations should carry out structured risk-based due diligence before engaging contractors or third parties.

Where appropriate contracts and service level agreements should include clear accountabilities for managing fraud risk and include termination provisions if a third party breaches its fraud management obligations.

Staff with responsibilities for managing contractors and third parties need a demonstrated high level of awareness of the particular fraud risks they face. Position descriptions and/or performance agreements for these roles could include responsibility for managing fraud risks.

24. Effective third party internal controls

Internal controls are integral to the fraud control framework. Specific internal controls relating to third parties should be in place, including auditing third party processes and transactions. Organisations should regularly carry out checks and reviews on their dealings with third parties.

The Audit Office's 2014 Better Practice Contract Management Framework provides guidance on internal controls in contract management arrangements.

25. Third party awareness and reporting

Contractors and suppliers need to understand that an organisation will not tolerate corruption, including fraudulent dealings. An organisation can use its statement of business ethics to set out expected standards and the mutual obligations of all parties.

Establishing reporting mechanisms and policies is important so that third parties have the same access to reporting systems as staff, including a hotline, online and email. Contractors and supppliers should be encouraged to provide information if they suspect fraud is occuring.

26. Staff disclosure of conflicts of interest and secondary employment

Staff should be required to disclosure conflicts of interest and secondary employment, which are recorded in a register. Registers need to be kept up to date and regularly reviewed so perceived or actual conflicts of interest can be properly managed.

Staff should be asked to complete a conflict of interest declaration annually and to confirm/reconfirm secondary employment requests at least every two years.

The fraud control framework

Attribute eight: Notification systems

Checklist

27. Culture that supports staff reporting fraud and management acting on those reports:

- ❒ well publicised options for staff to report fraud
- ❒ staff feel confident they will be protected from reprisal action
- ❒ demonstrated action taken in response to reports of fraud.

28. Polices, systems and procedures that support reporting:

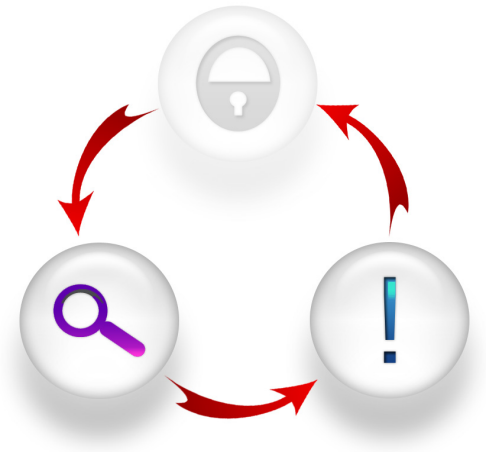
- ❒ reporting system appropriate to organisation
- ❒ different channels available to report fraud
- ❒ feedback and follow up with internal reporters.

29. Processes to support upward reporting:

- ❒ actual and suspected frauds reported to CEO and audit and risk committee
- ❒ fraud database published on organisation's website.

30. External reporting:

- ❒ staff are clear on policy and procedures for external reporting
- ❒ external reporting in accordance with legislation and policy
- ❒ clear and consistent approach to external reporting.



Resources – Fraud Control Health Check (resource three).

Employees and external parties should be encouraged to report unethical behaviour, including fraud. It is important for employees to be able to make such reports without fear of reprisal and with confidence the report will be taken seriously and acted upon.

The following elements support effective reporting.

27. Culture that supports staff reporting fraud and management acting on those reports

Staff (including consultants, contractors and suppliers) need to feel comfortable reporting unethical behaviour and have confidence the organisation will address complaints genuinely and protect reporters from reprisals. To provide this safe environment, an organisation needs well publicised options for reporting that accommodate the circumstances of the reporter and the nature of the complaint (for example, a hotline, email, online, option for anonymous reporting) as well as options for reporting to line managers or other nominated staff.

An organisation should be able to demonstrate it actively responds to reports of fraud. This includes giving feedback to the internal reporter (even if the action taken cannot be revealed, it is important for the reporter to know action has been taken) and publishing reports of fraud and responses on the organisation's website. Organisations should follow up with internal reporters to find out if they were satisfied with the actions taken and if not, identify areas for improvement.

28. Polices, systems and procedures that support reporting

Having appropriate systems and policies in place facilitates reporting by staff, consultants, contractors, customers and suppliers. The reporting system should be appropriate for the organisation's size and structure. For example, large complex organisations with a high inherent fraud risk may set up a reporting hotline, while geographically diverse organisations may appoint someone to receive reports in each location, as well as providing the means to make reports online or by email.

Staff need to be confident the organisation's culture supports honest and transparent reporting with a constructive approach to resolving problems and issues. Reporting systems should be established and supported by strong leadership and ethical frameworks – see attributes one and two.

Staff may be reluctant to report suspicions of fraud if they feel that no action will be taken in response to their allegations. As far as possible, an organisation should demonstrate the action it has taken and follow up directly with internal reporters.

Staff may feel more comfortable reporting fraud to their line manager, rather than an unknown individual. Managers require training on the organisation's policies for reporting allegations of fraud and how to deal with such reports.

Organisations must have policies and procedures for reporting public interest disclosures and there should be links between different reporting policies and channels.

29. Processes to support upward reporting

Actual or suspected frauds need to be reported to the CEO and audit and risk committee. This should be a standing item on the audit and risk committee's agenda.

It is important for an organisation to keep its fraud database current and published on its website. Before publishing fraud data, organisations should be satisfied that the publication will not prejudice an ongoing investigation.

The database should be used to report fraud and inform other business processes. It should capture all incidents and whether they were referred to an oversight agency or other body.

30. External reporting

It is important that policies on external reporting emphasise to staff the seriousness of fraud and the importance of actual and suspected fraud being reported to external bodies (including the NSW Police Force and the Independent Commission Against Corruption (ICAC)).

The principal officer of a public authority has an obligation to report corrupt conduct (which includes fraud) to the ICAC (s.11 of the *Independent Commission Against Corruption Act 1988*) and organisations must ensure external reporting is timely, accurate and compliant with legislation.

Staff should also be aware of the provision in s. 316(1) of the *Crimes Act 1900* which says in certain circumstances, failure to report a serious offence (which could include fraud) is an offence.

Organisations should take a clear and consistent approach to external reporting and detail in policies and procedures when reports will be made to external bodies.

The fraud control framework

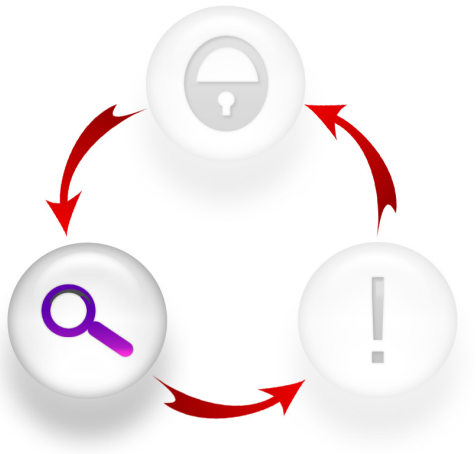
Attribute nine: Detection systems

Checklist

31. Robust internal controls:
- ❒ well documented risk-based internal controls
- ❒ routine checks of activities, processes, controls and transactions
- ❒ range of internal controls that 'prevent, detect and correct'.

32. Monitoring and review:
- ❒ available data monitored and reviewed to ensure irregularities and warning signals are picked up early
- ❒ early warning signs acted on quickly and red flag behaviour recognised.

33. Risk-based internal audit program:
- ❒ internal audit program evaluates the potential for fraud and how fraud risk is managed
- ❒ internal audit recommendations assigned to individuals with timeframes for response.



Resources – Fraud Control Health Check (resource three), Procurement Checklist (resource six).

It is important for an organisation to take ownership of its fraud risk and implement effective detection systems to mitigate these risks. An organisation should have:

31. Robust internal controls

Internal controls are an effective way to detect fraud. They should be well documented and risk focused. Organisations need to maintain adequate internal controls particularly during periods of change. Staff need to understand internal control processes are an essential part of the business and are in place to minimise errors and fraud, not because of a lack of trust.

Organisations should undertake routine checks of activities, processes, controls and transactions. Internal controls are designed to either 'prevent, detect or correct' and typically include:

- segregation of duties in high risk areas, such as procurement and payroll

  segregation of duties seeks to ensure no employee or group can perpetrate and conceal errors or fraud in the normal course of their duties. Generally, duties to be segregated are:
  - custody of cash/assets
  - authorisation or approval of related transactions affecting those assets
  - recording or reporting of related transactions
- personnel rotation
- staff taking at least two weeks recreation leave annually, particularly in high risk roles
- regular reviews and checks to detect irregularities:
  - as a routine part of regular line management
  - independently of line management via the audit and risk committee
- data mining
- post transaction reviews
- analysis of management accounts/ financial statements.

These controls should be supported by a culture of learning and continuous improvement. For example, an internal control review should occur after a fraud incident, during changes in business processes or functions and/ or when introducing new IT systems.

32. Monitoring and review

Organisations should thoroughly monitor and review available data to ensure irregularities and warning signals are picked up early and acted on quickly. Similarly organisations should learn to recognise red flag behaviours, such as unwillingness to take leave, unusually close relationships with suppliers, inconsistent financial reporting or unusually high overheads.

33. Risk-based internal audit program

The PSC's 'Behaving Ethically' guide at page 103 states 'agencies should have documented internal audit and fraud control systems in place, which are subject to ongoing monitoring and review as a matter of course'.

The NSW Treasury 'Internal Audit and Risk Management Policy for the NSW Public Sector (TPP 09-05)' states internal audit has a responsibility to:

- evaluate the potential for the occurrence of fraud and how the organisation manages fraud risk
- assist management to investigate fraud and identify the risks of fraud
- assist management to develop fraud prevention and monitoring strategies.

Importantly, internal audit recommendations need to be followed up, with responsibility assigned to individuals and clear time tables set for response. The outcomes of internal audits should be reported to management and the audit and risk committee.

Senior management and the audit and risk committee should regularly review the internal audit program. The audit and risk committee should have oversight of the process and make risk based recommendations on the systems to be audited.

The fraud control framework

Attribute ten: Investigation systems

Checklist

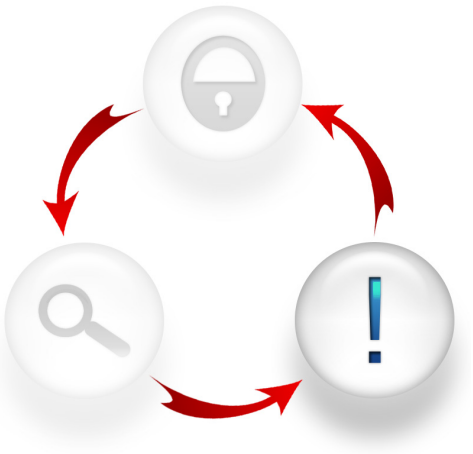
34. Clear documented investigation procedures:
- ❒ reports of fraud investigated promptly and to the highest standards
- ❒ investigations are independent
- ❒ sufficient resources allocated, including budget.

35. Investigations conducted by qualified and experienced staff:
- ❒ investigations conducted by appropriately qualified personnel with recognised qualifications and appropriate experience.

36. Decision-making protocols:
- ❒ documented decision-making processes
- ❒ proportionate responses to incidents of fraud.

37. Disciplinary systems:
- ❒ staff understand fraud will not be tolerated and the perpetrators will face disciplinary action
- ❒ commitment to taking action against the perpetrators of fraud
- ❒ consistent application of sanctions.

38. Insurance:
- ❒ consider a fidelity guarantee insurance policy to protect against the financial consequences of fraud.



Resources – Fraud Control Health Check (resource three).

Investigation is typically the last stage of the fraud control framework. If done badly the investigation can undermine the whole fraud control framework. Key to successful investigations systems are:

34. Clear, documented investigation procedures

Reports of fraud should be investigated promptly and to the highest standards of quality, using appropriate data gathering techniques and analysis. Prosecutions and disciplinary actions should not fail because of poor collection of evidence or other failures in the investigative process. Investigations must be independent and must not be undertaken by personnel with a conflict of interest in the matter. Sufficient resources, including budget, should be allocated.

Investigations should be reviewed by management and the audit and risk committee for procedural fairness and the results of investigations should be reported back to the internal reporter, where possible.

35. Investigations conducted by qualified and experienced staff

Depending on the nature of the alleged fraud, the size and structure of the organisation and the experience of internal staff, it may be appropriate for the investigation to be conducted by an external party. Regardless of whether an investigation is handled internally or externally, it needs to be conducted by appropriate personnel with recognised qualifications, such as a Certificate IV in Government (Investigation), and appropriate experience.

A suitable person within the organisation should be appointed to oversee any investigations that are carried out by an external party.

36. Decision-making protocols

Organisations should document decision making processes and apply graduated and proportionate responses to incidents of fraud. Organisations should have documented procedures for decision making, which are mindful of privacy principles and public interest disclosure protections.

Organisations need to document how to handle allegations of fraud, including the assessment of allegations, establishment of investigations and options for resolving incidents.

37. Disciplinary systems

Staff need to understand fraud will not be tolerated and the perpetrators will face disciplinary action.

Taking action against the perpetrators of fraud is key to an organisation's approach to fraud control. There should be a policy on termination of employment or other sanctions as well as a commitment to recovery action.

Importantly, sanctions should be seen to be applied consistently across the organisation with as much transparency around the process as possible.

38. Insurance

In line with AS 8001-2008, organisations need to consider holding a fidelity guarantee insurance policy to protect against the financial consequences of fraud. Holding such a policy should be subject to an ongoing cost/benefit analysis.

audit office
OF NEW SOUTH WALES

Appendix

Fraud Control Resources

These resources are designed to provide practical tools for organisations to help implement an effective fraud control framework. The resources can be adapted to suit particular circumstances. They are a guide only and should be supplemented by organisation-specific resources. In particular, organisations are encouraged to develop case studies and relevant practical examples for use in policies and educational material.

Resource one: Fraud control checklist

Attribute 1: Leadership

1. CEO and senior management commitment to fraud control:

- ❑ CEO visibly endorses fraud control activities
- ❑ senior managers demonstrate their commitment to mitigate fraud risks.

2. Clearly defined CEO and senior management accountability and responsibility:

- ❑ senior management assigned responsibility for implementing the fraud control framework
- ❑ senior managers' individual performance agreements contain performance measures and indicators relating to successful fraud control.

Attribute 2: Ethical framework

3. Clear policies setting out acceptable standards of ethical behaviour:

- ❑ staff have easy access to all ethical behaviour policies
- ❑ ethical behaviour policies are included in the induction process.

4. Demonstrated compliance with the ethical framework:

- ❑ staff annually evidence their commitment to acceptable standards of behaviour.

5. Employees can articulate obligations to ethical behaviour and the organisation's position on fraud:

- ❑ staff understand fraud is not tolerated and the consequences of committing fraud.

Attribute 3: Responsibility structures

6. Management and all staff have clearly defined responsibilities for managing fraud:

- ❑ staff are aware of the responsibility structure in the organisation
- ❑ responsibilities for fraud control are contained in role descriptions, where appropriate.

7. Fraud management is integrated with core business:

- ❑ managing fraud risks included in business plans.

8. Resources are allocated to managing fraud.

- ❑ fraud committee established and/or a Fraud Prevention Manager appointed.

9. Clearly defined roles for audit and risk committee and auditors:

- ❑ proactive and influential audit and risk committee
- ❑ internal audit work covers controls over high risk fraud areas.

10. Staff with responsibility for fraud control and staff in high risk fraud areas are provided with training:

- ❑ refresher and knowledge update training are provided on an ongoing basis
- ❑ training program is integrated within a wider education and awareness campaign.

Attribute 4: Fraud control policy

11. Risk-based policies appropriate to the organisation:

- ❑ appropriate policies address the level and nature of internal and external fraud risks
- ❑ fraud control policy addresses the ten attributes of fraud control.

12. Holistic and integrated:

- ❑ fraud control policy does not operate in isolation and has strong links to other ethical behaviour policies.

13. Regularly reviewed, current and implemented:

- ❑ fraud control policy is responsive to changes in the operating environment and reviewed at least every two years.

Attribute 5: Prevention systems

14. Proactive and integrated fraud risk assessment:

- ❑ fraud risk assessment is part of organisation's enterprise risk management process
- ❑ risk assessment reviewed after substantial change and at least every two years.

15. Planning, follow up and accountability:

- ❑ fraud control plan in place and outcomes reported to senior managers and audit and risk committee.

16. Analysis of and reporting on suspected and actual frauds:

- ❑ fraud database established containing all reports of fraud, action taken and outcomes
- ❑ database kept up to date and published on website.

17. Ethical workforce:

- ❑ pre-employment screening.

18. IT security strategy:

- ❑ specific IT security strategy aligned with the organisation's business strategy
- ❑ cybercrime included as a risk on the risk register.

Attribute 6: Fraud awareness

19. Comprehensive staff education and awareness program:

- ❑ ongoing ethical behaviour and fraud education and awareness program
- ❑ fraud control message repeated and reinforced using a variety of communication channels
- ❑ fraud control expectations included in the induction process
- ❑ staff have a good understanding of what fraud is
- ❑ guidance material deals with real life situations, conflicts and fraud risks staff face in their work area.

20. Staff awareness of fraud control responsibilities:

- ❑ staff have a good appreciation and understanding of their responsibilities for preventing, detecting and reporting fraud.

21. Customer and community awareness:

- ❑ publicity campaigns developed where appropriate
- ❑ customers and the community encouraged to report suspicions of fraud and provided with easy to use channels to make reports
- ❑ customers and the community have confidence in the integrity of the organisation
- ❑ statement of business ethics setting expectations and mutual obligations.

Attribute 7: Third party management systems

22. Targeted training and education for key staff:

- ❑ targeted training and education programs for staff with responsibilities for dealing with third parties.

23. Third party due diligence and clear contractual obligations and accountabilities:

- ❑ structured risk-based due diligence before engaging contractors or third parties
- ❑ contracts and service level agreements include clear accountabilities for managing the risk of fraud
- ❑ position descriptions for staff with responsibilities for managing third parties include accountabilities for managing fraud risks.

24. Effective third party internal controls:

- ❑ specific internal controls relating to third parties in place
- ❑ checks and reviews carried out on dealings with third parties.

25. Third party awareness and reporting:

- ❑ contractors and suppliers understand organisation will not tolerate corruption including fraudulent dealings
- ❑ statement of business ethics setting expectations and mutual obligations
- ❑ reporting mechanisms established for reporting suspected fraud
- ❑ contractors and suppliers encouraged to provide information if they suspect fraud is occurring.

26. Staff disclosure of conflicts of interest and secondary employment:

- ❑ staff regularly required to disclosure conflicts of interest and secondary employment
- ❑ records of conflicts of interest and secondary employment reviewed and kept up-to-date.

Attribute 8: Notification systems

27. Culture that supports staff reporting fraud and management acting on those reports:

- ❑ well-publicised options for staff to report fraud
- ❑ staff feel confident they will be protected from reprisal action
- ❑ demonstrated action taken in response to reports of fraud.

28. Polices, systems and procedures that support reporting:

- ❑ reporting system appropriate to organisation
- ❑ different channels available to report fraud
- ❑ feedback and follow-up with internal reporters.

29. Processes to support upward reporting:

- ❑ actual and suspected frauds reported to CEO and audit and risk committee
- ❑ fraud database published on organisation's website.

30. External reporting:

- ❑ staff are clear on policy and procedures for external reporting
- ❑ external reporting in accordance with legislation and policy
- ❑ clear and consistent approach to external reporting.

Attribute 9: Detection systems

31. Robust internal controls:

- ❑ well documented risk-based internal controls
- ❑ routine checks of activities, processes controls and transactions
- ❑ range of internal controls that 'prevent, detect and correct'.

32. Monitoring and review:

- ❑ available data monitored and reviewed to ensure irregularities and warning signals are picked up early
- ❑ early warning signs acted on quickly and red flag behaviour recognised.

33. Risk-based internal audit program:

- ❑ internal audit program evaluates the potential for fraud and how fraud risk is managed
- ❑ internal audit recommendations assigned to individuals with timeframes for response.

Attribute 10: Investigations systems

34. Clear documented investigation procedures:

- ❑ reports of fraud investigated promptly and to the highest standards
- ❑ investigations are independent
- ❑ sufficient resources allocated, including budget.

35. Investigations conducted by qualified and experienced staff:

- ❑ investigations conducted by appropriately qualified personnel with recognised qualifications and appropriate experience.

36. Decision-making protocols:

- ❑ documented decision-making processes
- ❑ proportionate responses to incidents of fraud.

37. Disciplinary systems:

- ❑ staff understand fraud will not be tolerated and the perpetrators will face disciplinary action
- ❑ commitment to taking action against the perpetrators of fraud
- ❑ consistent application of sanctions.

38. Insurance:

- ❑ consider a fidelity guarantee insurance policy to protect against the financial consequences of fraud.

Resource two: Risk assessment

This risk assessment gives an overview of the fraud risk assessment process and contains examples of the type of fraud risks and internal controls. Different organisations and different areas within your business may have different fraud risks and the examples are not an exhaustive checklist. The risk assessment deliberately does not include actual ratings for the effectiveness of internal controls, the results of the risk analysis, the options for the residual fraud risk or further treatment plans. Each organisation needs to undertake its own risk analysis and determine its own risk appetite.

1. Type of fraud risk

This column should include the potential fraud risks your organisation may face. Please specify any additional risks in the relevant section.

2. Existing controls

Once the potential fraud risks are identified, identify what controls currently exist to reduce each fraud risk.

3. Effectiveness of the existing controls

Assess how well controls are operating and if they are mitigating fraud risks as intended. Only one rating should be made for each fraud risk taking into consideration all controls existing for that risk. A scale of 1 to 5 is used.

1	There is a very high exposure to fraud (almost certain)
2	There is a high opportunity for fraudulent activity (likely)
3	There is a moderate opportunity for fraudulent activity (possible)
4	There is a low opportunity for fraudulent activity (unlikely)
5	There is no apparent opportunity for fraudulent activity (rare)

4. Fraud risk analysis

After considering how effective the controls are in step 3 above, the consequence and likelihood of each risk is assessed. By progressing in this order, this framework intends to assess the identified fraud risks on a residual basis, that is, after existing controls.

Impact / Probability	Insignificant	Minor	Moderate	Major	Catastrophic
Almost Certain	**Medium**	**Medium**	**High**	**Extreme**	**Extreme**
Likely	**Low**	**Medium**	**High**	**Extreme**	**Extreme**
Possible	**Low**	**Low**	**Medium**	**High**	**Extreme**
Unlikely	**Low**	**Low**	**Low**	**Medium**	**High**
Rare	**Low**	**Low**	**Low**	**Low**	**High**

5. Option for residual fraud risk

After considering the internal controls, determine if the residual fraud risk is at an acceptable level. If the residual fraud risk is acceptable, then there is no need for further action.

However if either:

(a) properly designed controls are not in place to address certain fraud risks, or
(b) controls identified are not operating effectively to sufficiently reduce the residual risk to an acceptable level

then action must be taken.

6. Further treatment/action necessary to address residual fraud risk

Where further action must be taken, the response should be to change or enhance existing controls or to implement additional controls.

FRAUD RISK ASSESSMENT								
Type of Fraud Risk	**Applicable to your area?** **Yes/No**	**Existing Controls**	**Effectiveness of Existing Controls (scale 1-5:)**	**Fraud Risk Analysis* (after existing controls)**			**Option for Residual Fraud Risk – Accept or Treat**	**Further Treatment/ Action (if necessary) to Address Residual Fraud Risk**
				Fraud Impact Rating	**Fraud Probability Rating**	**Residual Fraud Risk Rating**		
Identify individual fraud risks	*Yes* *No*	*Set out existing controls to mitigate the risk*	*How effective are the controls – refer to point 3 above*	*Insignificant* *Minor* *Moderate* *Severe* *Catastrophic*	*Almost certain* *Likely* *Possible* *Unlikely* *Rare*	*Low* *Medium* *High* *Extreme*	*Accept* *Treat*	*What additional action is necessary to treat the fraud risk?*
1. Falsifying working papers								
Falsifying working papers (annual report, document management system records and other documentation)		• Hierarchy of review of annual report • Audit and risk committee review annual report • Records management security						
False recordings on timesheets		• Manager approval of all timesheets • Staff made aware of overtime and flexible working policy and available on intranet						

FRAUD RISK ASSESSMENT

Type of Fraud Risk	Applicable to your area? Yes/No	Existing Controls	Effectiveness of Existing Controls (scale 1-5:)	Fraud Risk Analysis* (after existing controls)			Option for Residual Fraud Risk – Accept or Treat	Further Treatment/ Action (if necessary) to Address Residual Fraud Risk
				Fraud Impact Rating	Fraud Probability Rating	Residual Fraud Risk Rating		
Not submitting leave form		• Managers responsible to track and follow up delegated staff • Reconciliation between records performed by HR • Staff made aware of leave policy and procedures and they are available on intranet						
False overtime claims		• Manager approval of all timesheets • Manager review of overtime reports • Staff made aware of overtime and flexible working policy and available on intranet • Overtime approved in advance						

FRAUD RISK ASSESSMENT								
Type of Fraud Risk	**Applicable to your area? Yes/No**	**Existing Controls**	**Effectiveness of Existing Controls (scale 1-5:)**	**Fraud Risk Analysis* (after existing controls)**			**Option for Residual Fraud Risk – Accept or Treat**	**Further Treatment/ Action (if necessary) to Address Residual Fraud Risk**
				Fraud Impact Rating	**Fraud Probability Rating**	**Residual Fraud Risk Rating**		
2. Fraud in Hiring Contractors or Consultants								
Appointing contractors/consultants not supported by proper process		• Procurement policy and process exist, conform to NSW Procurement Framework and followed • Formal process of background checking • Appropriate levels of approval (for example, by management committees)						
Payments to contractors/consultants when work not performed or not performed satisfactorily		• Appropriate levels of authorisation assigned to senior management • Formal process of checking work performed against work plans and contracts prior to authorisation of payment						
3. Procurement Fraud *See resource 6*								

FRAUD RISK ASSESSMENT								
Type of Fraud Risk	**Applicable to your area? Yes/No**	**Existing Controls**	**Effectiveness of Existing Controls (scale 1-5:)**	**Fraud Risk Analysis* (after existing controls)**			**Option for Residual Fraud Risk – Accept or Treat**	**Further Treatment/ Action (if necessary) to Address Residual Fraud Risk**
				Fraud Impact Rating	**Fraud Probability Rating**	**Residual Fraud Risk Rating**		
4. Financial Fraud								
Theft of cash		• Adequate physical security over cash holdings, for example, access to safe and combination limited and safe locked. • The adequacy and validity of claims are checked • Regular reconciliation between cash counts, cash receipts and claims • Adequate building security and authorised issue and use of access passes						
Cheques made to false persons or companies		• The adequacy and validity of claims are checked • Claims not paid without authorisation • Segregation of duties						
EFT – payment to incorrect account or incorrect amount		• Claims not paid without review and authorisation • Segregation of duties						

FRAUD RISK ASSESSMENT

Type of Fraud Risk	Applicable to your area? Yes/No	Existing Controls	Effectiveness of Existing Controls (scale 1-5:)	Fraud Risk Analysis* (after existing controls)			Option for Residual Fraud Risk – Accept or Treat	Further Treatment/ Action (if necessary) to Address Residual Fraud Risk
				Fraud Impact Rating	Fraud Probability Rating	Residual Fraud Risk Rating		
Unrecorded transactions		• Regular reconciliation between cash counts, cash receipts and claims						
Unauthorised transactions		• Authorising staff member comply with delegated authority levels • Segregation of duties						
Transactions (expenditure/ receipts/deposits) recorded for incorrect sums		• Claims not paid without review and authorisation • Regular bank reconciliation performed • Receipts/deposits validated by supporting documentation						

FRAUD RISK ASSESSMENT								
Type of Fraud Risk	**Applicable to your area? Yes/No**	**Existing Controls**	**Effectiveness of Existing Controls (scale 1-5:)**	**Fraud Risk Analysis* (after existing controls)**			**Option for Residual Fraud Risk – Accept or Treat**	**Further Treatment/ Action (if necessary) to Address Residual Fraud Risk**
				Fraud Impact Rating	**Fraud Probability Rating**	**Residual Fraud Risk Rating**		
5. Personnel Fraud								
False person on payroll		• Copies of original documentation required to verify personal details of new staff, for example, copy of passport, birth certificate and tax documents • Comparing bank details to payroll records • Thorough reference checks carried out on new starters before appointment						
Overpay self or workmate each fortnight		• Regular management reviews of major cost fluctuations • Management authorisation of pay set-up • Staff are aware of overtime policy and available on intranet						

FRAUD RISK ASSESSMENT

Type of Fraud Risk	Applicable to your area? Yes/No	Existing Controls	Effectiveness of Existing Controls (scale 1-5:)	Fraud Risk Analysis* (after existing controls)			Option for Residual Fraud Risk – Accept or Treat	Further Treatment/ Action (if necessary) to Address Residual Fraud Risk
				Fraud Impact Rating	Fraud Probability Rating	Residual Fraud Risk Rating		
Re-direct employee's normal pay when resigned or on LWOP		• HR staff follow formally documented procedures surrounding change of bank details • Staff made aware of information security policy and available on intranet						
Pay self or workmate higher salary		• Regular management reviews of major cost fluctuations • Management authorisation of pay set up • Remuneration is determined within Award or Enterprise Agreement, available on intranet						

FRAUD RISK ASSESSMENT								
Type of Fraud Risk	**Applicable to your area? Yes/No**	**Existing Controls**	**Effectiveness of Existing Controls (scale 1-5:)**	**Fraud Risk Analysis* (after existing controls)**			**Option for Residual Fraud Risk – Accept or Treat**	**Further Treatment/ Action (if necessary) to Address Residual Fraud Risk**
				Fraud Impact Rating	**Fraud Probability Rating**	**Residual Fraud Risk Rating**		
6. Management Fraud								
Management fraud – manipulation of figures in management and financial reports (including annual report)		• Conflicts of interest are declared and registered • Conflicts of interest are managed appropriately and where a conflict arises, the manager is not involved in decision-making • Senior management and committee (audit, executive) reviews of management and financial reports • Audit of annual accounts • Internal and external audit						
Management fraud – using position to order goods and services for personal use		• Use of purchase guidelines and authorisation limits • Segregation of duties • All managers to sign code of conduct						
Writing off staff debts (as favour to workmates)		• All managers to sign code of conduct • Segregation of duties						

FRAUD RISK ASSESSMENT								
Type of Fraud Risk	**Applicable to your area? Yes/No**	**Existing Controls**	**Effectiveness of Existing Controls (scale 1-5:)**	**Fraud Risk Analysis* (after existing controls)**			**Option for Residual Fraud Risk – Accept or Treat**	**Further Treatment/ Action (if necessary) to Address Residual Fraud Risk**
				Fraud Impact Rating	**Fraud Probability Rating**	**Residual Fraud Risk Rating**		
7. Fraud involving assets or stores								
Equipment stolen or borrowed without permission		• Code of conduct promoted, available on intranet and signed by all staff • Secure storage of resources • Adequate building security and authorised issue and use of access passes • Staff made aware of information security policy and available on intranet						
Unauthorised use of cars/petrol cards/petrol		• Code of conduct promoted, available on intranet and signed by all staff • Staff made aware of motor vehicle and credit card policies and available on intranet • Management authorisation in line with delegations						

FRAUD RISK ASSESSMENT								
Type of Fraud Risk	**Applicable to your area? Yes/No**	**Existing Controls**	**Effectiveness of Existing Controls (scale 1-5:)**	**Fraud Risk Analysis* (after existing controls)**			**Option for Residual Fraud Risk – Accept or Treat**	**Further Treatment/ Action (if necessary) to Address Residual Fraud Risk**
				Fraud Impact Rating	**Fraud Probability Rating**	**Residual Fraud Risk Rating**		
Excessive private use of office equipment – for example, phones, copiers		• Code of conduct promoted, available on intranet and signed by all staff • Monitoring of usage and expenditure						
Using office resources to run a private business		• Code of conduct promoted, available on intranet and signed by staff • Monitoring of usage and expenditure						
8. Information Systems								
Fraud resulting from a loss of data following disaster or accident, for example, theft of assets not recorded		• Business continuity plan that is regularly reviewed • Saving working papers/documents in document management system or network drives that are regularly backed up • Regular back up and offsite storage of data • Staff made aware of information security policy and available on intranet						

FRAUD RISK ASSESSMENT

Type of Fraud Risk	Applicable to your area? Yes/No	Existing Controls	Effectiveness of Existing Controls (scale 1-5:)	Fraud Risk Analysis* (after existing controls)			Option for Residual Fraud Risk – Accept or Treat	Further Treatment/ Action (if necessary) to Address Residual Fraud Risk
				Fraud Impact Rating	Fraud Probability Rating	Residual Fraud Risk Rating		
Unauthorised staff accessing systems		• Appropriate level of computer access provided to staff • Staff reminded of responsibilities, for example, not to share passwords • Automatic log out of computers when extended period away from computer • System controls and checks						
Unauthorised release of user name and/or password		• Appropriate level of computer access provided to staff • Staff reminded of responsibilities, for example, not to share passwords						

FRAUD RISK ASSESSMENT

Type of Fraud Risk	Applicable to your area? Yes/No	Existing Controls	Effectiveness of Existing Controls (scale 1-5:)	Fraud Risk Analysis* (after existing controls)			Option for Residual Fraud Risk – Accept or Treat	Further Treatment/ Action (if necessary) to Address Residual Fraud Risk
				Fraud Impact Rating	Fraud Probability Rating	Residual Fraud Risk Rating		
Misrepresentation of the office by expressing personal views on office email, intranet or internet		• Policy on communication devices is signed by all employees • Code of conduct signed by all employees and available on the intranet • Disclaimers on all office emails						
Installation of illegal software on office computers and laptops		• Policy on communication devices is signed by all employees • Appropriate level of computer access provided to staff						

FRAUD RISK ASSESSMENT								
Type of Fraud Risk	**Applicable to your area? Yes/No**	**Existing Controls**	**Effectiveness of Existing Controls (scale 1-5:)**	**Fraud Risk Analysis* (after existing controls)**			**Option for Residual Fraud Risk – Accept or Treat**	**Further Treatment/ Action (if necessary) to Address Residual Fraud Risk**
				Fraud Impact Rating	**Fraud Probability Rating**	**Residual Fraud Risk Rating**		
9. Other fraud								
Selling, leaking or misusing information		• Code of conduct promoted, available on intranet and signed by all staff • Sound security maintained for sensitive and/or confidential information • Client and other confidential files locked away when not in use • Appropriate and timely storage or disposal of sensitive or confidential information • All staff given appropriate levels of access to client records and files • Sound IT controls • Staff made aware of information security policy and available on intranet						
Manipulating corporate and client information		• As above						

FRAUD RISK ASSESSMENT

Type of Fraud Risk	Applicable to your area? Yes/No	Existing Controls	Effectiveness of Existing Controls (scale 1-5:)	Fraud Risk Analysis* (after existing controls)			Option for Residual Fraud Risk – Accept or Treat	Further Treatment/ Action (if necessary) to Address Residual Fraud Risk
				Fraud Impact Rating	Fraud Probability Rating	Residual Fraud Risk Rating		
False travel/expense claims		• Code of conduct promoted, available on intranet and signed by all staff • Copy of invoices kept and management approval made for all expense claims • Segregation of duties						
Bribe accepted from clients, consultants or other service providers – for example, gifts, cash, event tickets and accommodation.		• Code of conduct promoted, available on intranet and signed by all staff • Staff made aware of gifts and benefits policy and is available on intranet						
Fraudulent claim for workers' compensation		• Follow formal procedures in dealing with a claim, for example, obtaining incident report and medical reports. • Suspected fraudulent workers' compensation claims reported and investigated						
False performance appraisal		• Review and approval of all appraisals by management						

FRAUD RISK ASSESSMENT

Type of Fraud Risk	Applicable to your area? Yes/No	Existing Controls	Effectiveness of Existing Controls (scale 1-5:)	Fraud Risk Analysis* (after existing controls)			Option for Residual Fraud Risk – Accept or Treat	Further Treatment/ Action (if necessary) to Address Residual Fraud Risk
				Fraud Impact Rating	Fraud Probability Rating	Residual Fraud Risk Rating		
False qualifications in job application		• Thorough reference checks carried out on new starters • Hiring staff (HR or unit team leaders) follow formally documented procedures • Interviews conducted by selection panel (two from business unit and one independent)						
Running a private business in office time		• Code of conduct promoted, available on intranet and signed by all staff • Review and approval of staff timesheets by management						
Running a private business/second job without permission		• Conflict of interest policy and secondary employment policy available on intranet and declaration signed by all staff						

FRAUD RISK ASSESSMENT

Type of Fraud Risk	Applicable to your area? Yes/No	Existing Controls	Effectiveness of Existing Controls (scale 1-5:)	Fraud Risk Analysis* (after existing controls)			Option for Residual Fraud Risk – Accept or Treat	Further Treatment/ Action (if necessary) to Address Residual Fraud Risk
				Fraud Impact Rating	Fraud Probability Rating	Residual Fraud Risk Rating		
Unauthorised access to office records including sensitive or confidential information and client information		• IT security (see Information Systems section eight above) • Limited records security and controls • Code of conduct promoted, available on intranet and signed by all staff						
Other (please specify)		•						
Other (please specify)		•						
Other (please specify)		•						

Resource three: Fraud control health check

The Fraud Control Health Check identifies:

- specific work areas where implementation of some elements of the organisation's fraud control framework may need refreshing or improving
- elements of the fraud control framework that may need attention across the entire organisation.

The health check consists of ten short and simple questions directed to staff. It should take no more than five minutes to complete, and responses are anonymous.

Who should be responsible for initiating the health check?

This health check is designed to assist organisations through their audit and risk committee (or equivalent). In organisations without an audit and risk committee or similar, the senior management team would take sole responsibility.

Audit and risk committees and senior management need a simple and effective way to review and monitor how effectively their organisations are implementing fraud control strategies. This health check has been developed to meet this requirement.

Audit and risk committees should initiate use of the Fraud Control Health Check on a regular basis. The frequency of use will depend on the nature of the fraud risks that the organisation faces in its internal and external environments.

If the organisation is exposed to significant levels of fraud risk overall, or if risk is high in particular work areas or functions, the health check may be used annually for areas presenting the greatest risks.

In other circumstances, we recommend that the health check be used at least once in all work areas across the organisation every two to three years.

For organisations exposed to moderate levels of fraud risk or greater, improving fraud control should be a standing item on the audit and risk committee's agenda.

How does the fraud control health check work?

The health check obtains the perceptions of staff about the fraud control environment in their specific work area. Based on that information, improvement action can be targeted as necessary.

The questions used derive from the Audit Office's updated 'ten attributes of fraud control' (first developed in 1994 and most recently updated in 2015).

Who should take responsibility for implementing the Fraud Control Health Check?

Responsibility for implementing and maintaining effective fraud control must always remain the responsibility of line management. However, there are also responsibilities for audit and risk committees.

Audit and risk committees and senior management must ensure that the Fraud Control Health Check is appropriately implemented across the organisation. Specifically, they will need to:

- tailor how this kit is used to suit the circumstances of the organisation
- decide how often the health check needs to be used
- assess whether to use the health check across the organisation as a whole or break it down over a two to three year cycle
- recommend improvement action to the CEO as suggested by the health check report
- report the results of the health check to the CEO, CFO and the organisation generally

- monitor the implementation of improvement actions identified.

There is a need for a project manager (this role could be assigned to the governance unit for example) to be designated to assist senior management and the audit and risk committee. The project manager will need to take responsibility for:

- making sure that the necessary activities take place throughout the organisation at the right time
- distributing the health check through the organisation (in line with the approach determined by the audit and risk committee)
- collecting the results of the health check and generating the report for the audit and risk committee.

How do you start?

The health check consists of ten short and simple questions directed to staff. The questionnaire should take an employee no more than five minutes to complete, and responses are anonymous.

The first decision required is, how often should the health check be used? This should be based on the nature and level of the fraud risks that the organisation faces in its internal and external environments.

Having determined the frequency to cover all work units, the second decision required is how many staff will be surveyed? While responses from ten to 20 per cent of total staff across the organisation would be sufficient, more views will provide greater insight. In small organisations, and in small work areas, it is better to survey all staff.

The health check process is quick and simple enough to use quite broadly. Processing and analysis is also simple and inexpensive.

The project manager will need to set up suitable arrangements for distribution and collection of the health check. A variety of sophisticated online survey tools are available and may already be used elsewhere within your organisation. Email is not recommended, as anonymity of responses is important.

What do you do with the results?

Questionnaire responses need to be entered into a spreadsheet. The spreadsheet generates a health check report that flags areas for attention using simple colour coding.

The report's format works in two ways. Firstly, it identifies particular work areas where staff perceptions of the fraud control environment suggest that some attention is warranted. Secondly, it flags specific attributes of the fraud control framework that appear to warrant some attention across the organisation.

Generating the health check report

Entering staff responses from the health check questionnaire into the spreadsheet is very straightforward. The colour coded fields and the 'overall results' columns update automatically to reflect the entries made.

The health check report generated from the spreadsheet looks like this:

Fraud Control Attribute	Overall Results for Individual Fraud Control Attributes	Results for Individual Work Areas			
		Work Area One	Work Area Two	Work Area Three	Work Area Four
1. Leadership	green	green	green	green	orange
2. Ethical framework	green	green	green	green	green
3. Responsibility structures	orange	green	orange	green	red
4. Fraud control policy	orange	green	green	orange	red
5. Prevention systems	red	orange	red	red	red
6. Fraud awareness	orange	green	orange	green	red
7. Third party management systems	green	orange	green	green	green
8. Notification systems	red	green	red	orange	red
9. Detection systems	green	green	green	green	orange
10. Investigation systems	green	green	green	green	green
Overall Work Area Results		green	orange	orange	red

Key

Good performance	green	Action required	orange	Urgent action required	red

How do you interpret the results?

Work areas or aspects of the fraud control framework that are flagged for attention by the health check report may have systemic problems (as in control gaps, for example), or staff awareness of the fraud control environment may simply need refreshing.

Either way, action is needed to ensure that ongoing implementation of the organisation's fraud control framework is effective.

The above sample report suggests that:

- staff in work area four have not sensed clearly defined and appropriate responsibility structures.
- the Fraud Control Improvement Workshop (resource four) should be run for that work area as a matter of priority
- staff in work areas two and three have mixed perceptions about the fraud control environment. Time and resources permitting, the Fraud Control Improvement Workshop should also be run in those work areas.
- fraud control attributes five and eight should be reviewed. Their implementation appears to be failing in some work areas. Those parts of the fraud control framework may need improvement (perhaps circumstances have changed). Or staff awareness about them may need refreshing (staff turnover and organisational change makes this a frequent issue requiring attention)
- fraud control attributes three, four and six would also benefit from review if resources and time are available. There are signs that the effectiveness of their implementation may be weakening.

What do you do when there are improvements needed?

After considering the health check report and making such further enquiries as felt necessary, senior management should:

- recommend action to the chief executive
- monitor actions and progress.

Circumstances will vary for each organisation, however, action would normally be recommended where the health check report shows red or amber in the 'overall results' section for:

- a particular work area
- a particular fraud control attribute.

For work areas that the health check has flagged for attention, recommended action would generally be for the work area to undertake the Fraud Control Improvement Workshop (resource four).

For attributes of the fraud control framework that require attention, recommended action would generally be to assign them to a relevant 'organisation owner' for action depending on the attribute of the fraud control framework needing attention.

The health check report generator

A blank pro-forma of the health check questionnaire to be distributed to staff is provided on the next page.

The spreadsheet to be used to input responses from staff is available for download from our website (no agency data is captured or retained by the Audit Office).

The spreadsheet can accommodate 20 work areas, each with 30 staff. Organisations can modify the spreadsheet or the questionnaire to suit their individual circumstances – in terms of the number of work areas, staff to be surveyed, or additional questions to be asked[1].

Extending use of the health check for benchmarking purposes

As part of an organisation's ongoing efforts to maintain and improve fraud control, it is recommended that the Fraud Control Health Check also be used for benchmarking purposes.

[1] Deletion of any questions, or modification of any of the underlying formulas and dashboard colour calibrations in the spreadsheet, is not permitted.

Internal benchmarking is the easiest to organise and could involve:

- benchmarking the performance of the organisation as a whole over time
- benchmarking the performance of individual work areas over time
- benchmarking across a number of individual work areas at a single point of time (where work areas share a common basis of operations but might be spread across different geographical areas)
- benchmarking across a number of individual work areas over time.

External benchmarking is harder to organise but has a range of significant benefits. In particular, the ability to learn from the experiences of other organisations has much to commend it.

External benchmarking could involve:

- benchmarking between similar organisations
- benchmarking between organisations that are in different fields. Benchmarking syndicates could provide interested organisations the opportunity to measure performance against a common standard and to learn about performance differences.

The Fraud Control Health Check questionnaire

Please put a tick in the most appropriate box	Strongly disagree	Disagree	Unsure	Agree	Strongly agree
The CEO and senior management team are committed to actively controlling fraud in my workplace					
We have ethical behaviours policies that most staff in my work area are aware of and understand that staff will be disciplined for fraudulent or corrupt behaviour, and for breaches of our code of conduct/ethics					
Most staff in my work area are aware of their responsibilities and the responsibilities of management for minimising fraud in our workplace					
Our fraud control policies and procedures tell us how to deal effectively with the fraud risks we face					
The functions of my work area are regularly assessed to identify and address the fraud risks we face					
Our organisation runs a comprehensive awareness program about fraud control					
I am confident our organisation has policies and systems in place to ensure that third parties are appropriately checked and verified					
Staff and third parties are encouraged to report alleged fraud or corruption in my organisation					
I am confident my organisation systematically makes efforts to detect fraud and corruption					
I am confident internal investigations of alleged fraud and corruption would be carried out independently and to high standards in my organisation					

Have you got any general comments about the fraud control environment in your work area?

Name of your work area (not YOUR name – your response is anonymous).

Resource four: Fraud control improvement workshops

The Fraud Control Improvement Workshops would be used only when and where this is suggested by the results shown in the management report generated from the Fraud Control Health Check.

How does the Fraud Control Improvement Workshop operate?

The Fraud Control Improvement Workshop is used after the Fraud Control Health Check (see resource three). It is used only for work areas where staff perceptions about the fraud control environment suggest that some attention is necessary. It will take the work area around two to three hours to run.

Work areas that are flagged for attention by the health check report may have systemic problems (as in control gaps, for example), or staff awareness of the fraud control environment may simply need refreshing. Either way, action is needed to ensure that ongoing implementation of the organisation's fraud control framework is effective.

The improvement workshop has been designed to:

- encourage structured, critical analysis and discussion about the current situation
- develop practical actions for implementation.

The improvement workshop gets staff to examine the fraud control environment, as they understand it, in some detail. This is done in a structured fashion, using the Audit Office's 'ten attributes of fraud control'.

How should the process be managed?

The decision about which work areas should run the workshop is made by the CEO.

Senior management and the audit and risk committee will monitor to ensure that workshops are conducted and that suitable action is taken as determined by each workshop.

Consider repeating the Fraud Control Health Check again (which takes staff only five minutes) after 12 months, in the work areas where the workshops were held, to ensure things have improved.

In setting up the workshops, the designated Project Manager will assist work areas to make the necessary arrangements. This includes determining the most appropriate person to serve as facilitator for the workshop (a role sometimes allocated to internal audit).

The facilitator will lead the work area through the process of discussion at the workshop, but ownership of issues and responsibility for results remains with the work area. The facilitator will assist the work area to reach conclusions and to resolve a plan of action that suits that particular situation.

What is needed to arrange the workshop, and how does it need to be run to be successful?

This workshop is a generic template that can be modified if an organisation desires[2].

The workshop is a directive from the CEO, so the work area manager should ensure that as many staff attend as possible – supervisory and management/executive staff included.

The facilitator will lead the workshop, and needs to ensure:

- there is effective participation from all staff at the workshop
- the knowledge of those attending is shared and harnessed. Sometimes this may be the most important contribution of the workshop. Some staff may be aware of issues, or rules and controls, which others are not. Staff in management positions may have knowledge of policies and systems that operational staff do not
- particular individuals, or those in management positions, do not dominate the time or directions of the workshop
- the discussions lead to a set of practical actions that can be taken to improve the fraud control environment at the work area.

In particular, participants must have the opportunity to change their ratings through the discussion process. The aim of this process is to discuss, share information and to critically reflect on issues. As such, people changing their views or ratings is a sign of success.

Staff may not be aware that the organisation has a formal fraud control framework, or of its various component parts (such as policies, rules and systems). But regardless of what staff know about specific corporate policies and systems, they will have developed perceptions about the fraud control environment that operates in practice at their work area. Those perceptions are very important. They are a reality test for the effective implementation of the organisation's fraud control framework.

The workshop will:

- make staff more aware of the things that the organisation has done to develop a fraud control environment that suits the risks it faces
- synthesise staff perceptions about the fraud control environment for their work area to identify how it can be improved.

This is done by systematically working through each of the elements of the fraud control framework, using the Audit Office's 'ten attributes of fraud control'.

For each of the ten attributes, the workshop provides participants with:

- an understanding of what the attribute is trying to achieve
- questions to think about, to help them more fully understand the issues
- an opportunity to think about and assess what may have been done previously to address the aspects involved for that attribute
- indicators of how to tell if the things that have been done to address that attribute are contributing to creating the desired type of fraud control environment at this work area
- an analysis of what could be done to improve things
- an assessment of who would undertake these actions, and when.

This may generate too many suggestions to be practical, so the final step is to focus upon a small number of key actions as immediate priorities.

2 Modifications to the workshop materials should be limited to minor variations and tailoring to suit local conditions, terminology etc.

Facilitator's guide

There are twelve mini-sessions in the workshop.

To start with, a general introduction and welcome is required to set the context. The previous sections of this document can be used as guidance material.

There is then a session for each of the ten fraud control attributes, and finally a summary session to prioritise a small number of key actions. Modules (worksheets) are attached to work through for each of these sessions.

For each module, the facilitator needs to:

- read through with the participants the aims of the attribute and issues to think about, and get them to make notes
- get participants to think about and make notes of any previous improvement initiatives and useful future directions
- generate group discussion of the above
- move the group on to rating current achievements for the attribute
- while it is important to read through the material together, it is important the assessment is made individually
- generate discussion about ratings. Discussing reasons for the rating is most important. Perhaps individuals could be chosen and asked to explain their view, and then for each other module ask a different person their opinion, or maybe there is opportunity for a show of hands to indicate the views of the group which are then compared and contrasted
- give participants an opportunity to re-think their rating in light of the discussion
- direct the group to the final question for each module, determining future actions. The group needs some time to answer this question individually and then to discuss their answers
- facilitate agreement about the actions required (if any), who will do them and when
- record the actions, who will do them and when for the group as a whole.

This will be the pattern for each of the ten attributes.

At the end of the workshop, the facilitator will need to review the aggregated actions with the group so that they can be given one last review for practicality, robustness, final changes, and so on.

Finally, it is better to pick, say, six key tasks to be done rather than trying to achieve each and every improvement action identified. A worksheet is provided for this.

What should be reported to management?

The facilitator will prepare a report for the Project Manager.

This need not be a lengthy document – it is more about reporting the improvement actions to be taken, who will be undertaking them and when.

The Project Manager will provide this information to senior management and the audit and risk committee, who will monitor the ongoing progress of action taken as determined by each workshop.

What else?

Reporting across the organisation of directions, strategies and actions to improve individual workplaces is vital. This is often the loop that is missing in the performance improvement process: reporting on, and monitoring, the outcomes of all the work undertaken as part of this process.

Fraud Control Improvement Workshop

Participant Worksheets

Leadership

Just so you know

This is attribute one (of ten) in your organisation's fraud control framework.

It is one of a number of elements that contribute to establishing a fraud control environment for the organisation.

This specific attribute would be working well if:

- **your CEO and senior management are visibly committed to fraud control**
- **your organisation has clearly defined CEO and senior management accountability and responsibility**
- **senior management assigned responsibility for implementing the fraud control framework**
- **senior managers' individual performance agreements contain performance measures and indicators relating to successful fraud control.**

Signs of success?

Please consider your own views about the following points. People in different roles and at different levels may have different knowledge and different views about these matters – that is fine. Just say what you think, based on what you know:

Do you perceive that your CEO is committed to managing fraud risk in your organisation?	
Do the CEO and senior managers set a clear tone at top concerning fraud control? Do they provide a good example?	
Do most staff in your work area know who within the organisation is responsible for implementing fraud control?	
Do most staff in your work area know who within the organisation is responsible for monitoring fraud control?	
Do you feel that senior management within your organisation see fraud control as a priority?	

Previous fraud control performance improvement initiatives

Can you think of any actions that have been taken in recent times (say, in the past year or so) to improve leadership around fraud control, either at your workplace or for the organisation generally? Jot down any that you can think of.

Rating current performance

Thinking about what this attribute is seeking to achieve, and the perceptions about those outcomes that you have developed through your experiences, how would you rate this aspect of the fraud control environment? Circle one.

Either: It is all news to me (I have never heard about it and see no signs that it exists) *or* it is clearly not working	Ok at best, but it's not very clear to me that it is working well	Seems quite good	Yes, it is clear to me that it is working very well
Score 1	Score 2	Score 3	Score 4

So the group can discuss this, please make a few notes of the main reasons that have lead you to give this rating.

Your workshop facilitator will get the group to discuss the various ratings that people came up with, and why. This may bring things to your attention that you were not aware of, or help you to clarify your thinking.

After discussion, if you want to reassess the rating that you made, this is fine.

The facilitator will seek to reach a group consensus on the rating, but this is not vital.

Determining Future Actions

For this attribute (only) of the fraud control framework, does your workplace, and/or the organisation, need to do something to improve the situation NOW? (Other things that you think may need to be done will be covered later under the other attributes.) *Please circle one.*

If 'yes', please make some notes below about:

- *what are the things that need to be done?*
- *who do you think should do it?*
- *by when?*

What?	Who?	When?

The group will come back to these later, to work out a shortlist of the top priority actions.

Ethical framework

Just so you know

This is attribute two (of ten) in your organisation's fraud control framework.

It is one of a number of elements that contribute to establishing a fraud control environment for the organisation.

This specific attribute would be working well if:

- **your organisation has clear policies setting out acceptable standards of ethical behaviour**
- **staff have easy access to all ethical behaviour policies and these are included in induction process**
- **staff annually evidence their commitment to acceptable standards of behaviour**
- **employees can articulate their obligations to ethical behaviour and the organisation's position on fraud**
- **staff understand fraud is not tolerated and the consequences of committing fraud.**

Signs of success?

Please consider your own views about the following points. People in different roles and at different levels may have different knowledge and different views about these matters – that is fine. Just say what you think, based on what you know.

Are most of the staff in your work area aware of the ethical behaviour policies in your organisation?	
Do these policies give clear directions, strategies and actions to facilitate an ethical workplace?	
Are these policies used in a meaningful way to inform workplace practices?	
Are you able to explain what your obligations are under these policies?	
Are most staff in your work area clear about what fraud is, your organisation's stance on fraud, and the consequences of committing fraud?	

Previous fraud control performance improvement initiatives

Can you think of any actions that have been taken in recent times (say, in the past year or so) to improve the ethical framework, either at your workplace or for the organisation generally? Jot down any that you can think of.

Rating current performance

Thinking about what this attribute is seeking to achieve, and the perceptions about those outcomes that you have developed through your experiences, how would you rate this aspect of the fraud control environment?

Either: It is all news to me (I have never heard about it and see no signs that it exists) *or* it is clearly not working	Ok at best, but it's not very clear to me that it is working well	Seems quite good	Yes, it is clear to me that it is working very well
Score 1	Score 2	Score 3	Score 4

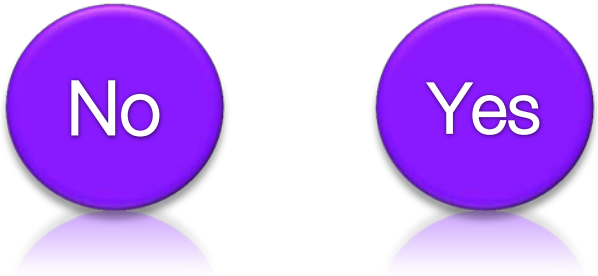
So that the group can discuss this, please make a few notes of the main reasons that have lead you to give this rating.

Your workshop facilitator will get the group to discuss the various ratings that people came up with, and why. This may bring things to your attention that you were not aware of, or help you to clarify your thinking.

After discussion, if you want to reassess the rating that you made, this is fine. The facilitator will seek to reach a group consensus on the rating, but this is not vital.

Determining Future Actions

For this attribute (only) of the fraud control framework, does your workplace, and/or the organisation, need to do something to improve the situation NOW? (Other things that you think may need to be done will be covered later under the other attributes.) *Please circle one.*



If 'yes', please make some notes below about:

- *what are the things that need to be done?*
- *who do you think should do it?*
- *by when?*

What?	Who?	When?

The group will come back to these later, to work out a shortlist of the top priority actions.

Responsibility structures

Just so you know

This is attribute three (of ten) in your organisation's fraud control framework.

It is one of a number of elements that contribute to establishing a fraud control environment for the organisation.

This specific attribute would be working well if:

- **management and all staff in your organisation have clearly defined responsibilities for managing fraud**
- **staff are aware of the responsibility structure in the organisation**
- **responsibilities for fraud control are contained in role descriptions where appropriate**
- **fraud management is integrated with core business**
- **fraud committee established and/or a fraud prevention manager appointed**
- **resources have been allocated to managing fraud**
- **there are clearly defined roles for audit and risk committee and auditors**
- **your audit and risk committee is proactive and influential**
- **staff with responsibility for fraud control and staff in high risk areas are provided with training.**
- **the training program is integrated within a wider education and awareness campaign**

Signs of success?

Please consider your own views about the following points. People in different roles and at different levels may have different knowledge and different views about these matters – that is fine. Just say what you think, based on what you know.

Do most staff in your work area know who within the organisation is responsible for implementing fraud control?	
Do most staff in your work area know who within the organisation is responsible for monitoring fraud control?	
Do most staff in your work area have an understanding of their own personal fraud control responsibilities?	
Is fraud control covered in any role descriptions in your work area?	
Are most staff in your work area aware of responsibilities for fraud control at your work area?	

Table continues over the page.

Is managing fraud part of your team plan and discussed in team or planning meetings?	
Have resources been allocated to managing fraud?	
Is there a fraud control committee and/or a fraud prevention manager?	
Is specific training provided to staff with responsibility to manage fraud?	

Previous fraud control performance improvement initiatives

Can you think of any actions that have been taken in recent times (say, in the past year or so) to improve the clarity of responsibility structures, either at your workplace or for the organisation generally? Jot down any that you can think of.

Rating current performance

Thinking about what this attribute is seeking to achieve, and the perceptions about those outcomes that you have developed through your experiences, how would you rate this aspect of the fraud control environment?

Either: It is all news to me (I have never heard about it and see no signs that it exists) *or* it is clearly not working	Ok at best, but it's not very clear to me that it is working well	Seems quite good	Yes, it is clear to me that it is working very well
Score 1	Score 2	Score 3	Score 4

So the group can discuss this, please make a few notes of the main reasons that have lead you to give this rating.

Your workshop facilitator will get the group to discuss the various ratings that people came up with, and why. This may bring things to your attention that you were not aware of, or help you to clarify your thinking.

After discussion, if you want to reassess the rating that you made, this is fine.

The facilitator will seek to reach a group consensus on the rating, but this is not vital.

Determining Future Actions

For this attribute (only) of the fraud control framework, does your workplace, and/or the organisation, need to do something to improve the situation NOW? (Other things that you think may need to be done will be covered later under the other attributes.) *Please circle one.*

If 'yes', please make some notes below about:

- *what are the things that need to be done?*
- *who do you think should do it?*
- *by when?*

What?	Who?	When?

The group will come back to these later, to work out a shortlist of the top priority actions.

Fraud control policy

Just so you know
This is attribute four (of ten) in your organisation's fraud control framework.

It is one of a number of elements that contribute to establishing a fraud control environment for the organisation.

This specific attribute would be working well if:

- **your organisation has a risk-based fraud control policy which is appropriate to your organisation**
- **your organisation's fraud control policy addresses the ten attributes of fraud control**
- **your organisation's fraud control policy is integrated within a wider ethical framework and is linked to other ethical behaviours policies**
- **the policy is responsive to changes in the operating environment and reviewed at least every two years**

Signs of success?
Please consider your own views about the following points. People in different roles and at different levels may have different knowledge and different views about these matters – that is fine. Just say what you think, based on what you know.

Are most staff in your work area aware of the main policy elements involved with the fraud control policy?	
Is your fraud control policy integrated within a wider ethical framework and linked to other ethical behaviour policies?	
How relevant and up to date is the policy in its current form?	
Is it your perception that the policy sits on a shelf or do you see that is it a living document that is used as a reference for dealing meaningfully with this issue?	
How clear is the policy? Does it give clear directions, strategies and actions to drive fraud control at your workplace?	

Table continues over the page.

Does the policy adequately cover the risks for your workplace?	
Are there gaps or elements in need of improvement in the policy?	

Previous fraud control performance improvement initiatives

Can you think of any actions that have been taken in recent times (say, in the past year or so) to improve fraud policies, systems and procedures, either at your workplace or for the organisation generally? Jot down any that you can think of.

Rating current performance

Thinking about what this attribute is seeking to achieve, and the perceptions about those outcomes that you have developed through your experiences, how would you rate this aspect of the fraud control environment?

Either: It is all news to me (I have never heard about it and see no signs that it exists) *or* it is clearly not working	Ok at best, but it's not very clear to me that it is working well	Seems quite good	Yes, it is clear to me that it is working very well
Score 1	Score 2	Score 3	Score 4

So that the group can discuss this, please make a few notes of the main reasons that have lead you to give this rating.

Your workshop facilitator will get the group to discuss the various ratings that people came up with, and why. This may bring things to your attention that you were not aware of, or help you to clarify your thinking.

After discussion, if you want to reassess the rating that you made, this is fine.

The facilitator will seek to reach a group consensus on the rating, but this is not vital.

Determining Future Actions

For this attribute (only) of the fraud control framework, does your workplace, and/or the organisation, need to do something to improve the situation NOW? (Other things that you think may need to be done will be covered later under the other attributes.) *Please circle one.*

If 'yes', please make some notes below about:

- *what are the things that need to be done?*
- *who do you think should do it?*
- *by when?*

What?	Who?	When?

The group will come back to these later, to work out a shortlist of the top priority actions.

Prevention systems

Just so you know

This is attribute five (of ten) in your organisation's fraud control framework.

It is one of a number of elements that contribute to establishing a fraud control environment for the organisation.

This specific attribute would be working well if:

- your organisation undertakes regular assessments of its fraud risks
- the risk assessment is reviewed after substantial change and at least every two years
- your organisation takes action to mitigate the risks identified, assigns responsibility and holds people to account
- there is a fraud control plan in place
- your organisation analyses reports of suspected and actual frauds and reports publically on the outcomes
- there is pre-employment screening process in place
- your organisation has developed a specific IT security strategy.

Signs of success?

Please consider your own views about the following points. People in different roles and at different levels may have different knowledge and different views about these matters – that is fine. Just say what you think, based on what you know.

Has your organisation assessed its fraud risks?	
Has fraud risk been assessed within the past two-three years?	
Have fraud risks been formally identified at your work area?	
Has responsibility for mitigating these risks been assigned?	
Have fraud controls been discussed in your work area?	
Does your organisation have a fraud control plan?	
Does your organisation have a fraud database published on its website?	
Does your organisation conduct pre-employment screening?	
Does your organisation have an IT security strategy in place?	

Previous fraud control performance improvement initiatives

Can you think of any actions that have been taken in recent times (say, in the past year or so) to improve the prevention systems, either at your workplace or for the organisation generally? Jot down any that you can think of.

Rating current performance

Thinking about what this attribute is seeking to achieve, and the perceptions about those outcomes that you have developed through your experiences, how would you rate this aspect of the fraud control environment?

Either: It is all news to me (I have never heard about it and see no signs that it exists) *or* it is clearly not working	Ok at best, but it's not very clear to me that it is working well	Seems quite good	Yes, it is clear to me that it is working very well
Score 1	Score 2	Score 3	Score 4

So that the group can discuss this, please make a few notes of the main reasons that have lead you to give this rating.

Your workshop facilitator will get the group to discuss the various ratings that people came up with, and why. This may bring things to your attention that you were not aware of, or help you to clarify your thinking.

After discussion, if you want to reassess the rating that you made, this is fine.

The facilitator will seek to reach a group consensus on the rating, but this is not vital.

Determining Future Actions

For this attribute (only) of the fraud control framework, does your workplace, and/or the organisation, need to do something to improve the situation NOW? (Other things that you think may need to be done will be covered later under the other attributes.) *Please circle one.*

If 'yes', please make some notes below about:

- *what are the things that need to be done?*
- *who do you think should do it?*
- *by when?*

What?	Who?	When?

The group will come back to these later, to work out a shortlist of the top priority actions.

Fraud awareness

Just so you know

This is attribute six (of ten) in your organisation's fraud control framework.

It is one of a number of elements that contribute to establishing a fraud control environment for the organisation.

This specific attribute would be working well if:

- your organisation runs a comprehensive staff education and awareness program
- fraud control expectations are included in the induction process
- fraud control message is repeated and reinforced using a variety of communication channels
- staff have a good understanding of what fraud is.
- guidance material deals with real life situations, conflicts and fraud risks that staff face in their work area
- staff have a good appreciation and understanding of their responsibilities for preventing, detecting and reporting fraud
- publicity campaigns are developed where appropriate
- customers and the community are encouraged to report suspicions of fraud and provided with easy to use channels to make reports
- customers and the community have confidence in the integrity of the organisation
- your organisation has a statement of business ethics setting expectations and mutual obligations

Signs of success?

Please consider your own views about the following points. People in different roles and at different levels may have different knowledge and different views about these matters – that is fine. Just say what you think, based on what you know.

Do most staff in your work area understand their fraud control responsibilities?	
Have you seen actions by your colleagues that show they are clear about it?	
Has action been taken by corporate or local management to encourage staff to be active about fraud control?	
Do staff get mixed messages about the organisation's values and expectations concerning fraud control?	
Has fraud control training been provided in the recent past?	

Table continues over the page.

Are there visible reminders about corruption prevention and ethics in your work area?	
Is fraud control guidance material for staff available? Is it useful and up-to-date?	
Is there highly visible information displayed for customers at your work area about your organisation having a strong anti-fraud stance?	
Are community and customers encouraged to provide information if they suspect fraud/corruption?	
Does your organisation's annual report contain a strong anti-fraud message and details of any frauds reported during the year?	
Does your organisation's annual report contain details of its fraud control framework, including its values, code of conduct, prevention/ detection/investigation elements?	
What do you think the community's view would be of your organisation's integrity?	

Previous fraud control performance improvement initiatives

Can you think of any actions that have been taken in recent times (say, in the past year or so) to improve fraud awareness, either at your workplace or for the organisation generally? Jot down any that you can think of.

Rating current performance

Thinking about what this attribute is seeking to achieve, and the perceptions about those outcomes that you have developed through your experiences, how would you rate this aspect of the fraud control environment?

Either: It is all news to me (I have never heard about it and see no signs that it exists) *or* it is clearly not working	Ok at best, but it's not very clear to me that it is working well	Seems quite good	Yes, it is clear to me that it is working very well
Score 1	Score 2	Score 3	Score 4

So the group can discuss this, please make a few notes of the main reasons that have lead you to give this rating.

Your workshop facilitator will get the group to discuss the various ratings that people came up with, and why. This may bring things to your attention that you were not aware of, or help you to clarify your thinking.

After discussion, if you want to reassess the rating that you made, this is fine.

The facilitator will seek to reach a group consensus on the rating, but this is not vital.

Determining Future Actions

For this attribute (only) of the fraud control framework, does your workplace, and/or the organisation, need to do something to improve the situation NOW? (Other things that you think may need to be done will be covered later under the other attributes.) *Please circle one.*

If 'yes', please make some notes below about:

- *what are the things that need to be done?*
- *who do you think should do it?*
- *by when?*

What?	Who?	When?

The group will come back to these later, to work out a shortlist of the top priority actions

Third party management systems

Just so you know
This is attribute seven (of ten) in your organisation's fraud control framework.

It is one of a number of elements that contribute to establishing a fraud control environment for the organisation.

This specific attribute would be working well if:

- **there is targeted training and education for staff with responsibilities for dealing with third parties**
- **your organisation carries out structured risk-based due diligence before engaging contractors or third parties**
- **contracts and service level agreements include clear accountabilities for managing the risk of fraud**
- **position descriptions for staff with responsibilities for managing third parties include accountabilities for managing fraud risks**
- **your organisation carries out checks and reviews on their dealings with third parties**
- **contractors and suppliers understand your organisation will not tolerate corruption including fraudulent dealings**
- **your organisation's statement of business ethics sets expectations and mutual obligations**
- **reporting mechanisms are established for reporting suspected fraud**
- **contractors and suppliers are encouraged to provide information if they suspect fraud is occurring**
- **staff are required to regularly disclose conflicts of interest and secondary employment**
- **records of conflicts of interest and secondary employment reviewed and kept up to date.**

Signs of success?
Please consider your own views about the following points. People in different roles and at different levels may have different knowledge and different views about these matters – that is fine. Just say what you think, based on what you know.

Are staff in key areas provided with specialist training on managing the fraud risks involved with dealing with third parties?	
Is it your perception that your organisation carries out checks on its suppliers and contractors?	

Table continues over the page.

Does your organisation have a statement of business ethics or equivalent which third parties are expected to comply with?	
Are contractors and suppliers formally provided with material that indicates a strong anti-fraud stance by your organisation?	
Does your organisation have ways for third parties to report suspected fraud, i.e. is there a hotline, email contact or an online form?	
Are contractors and suppliers actively encouraged to report suspected fraud?	
Does your organisation have a conflicts of interest policy and secondary employment policy?	
Are you regularly asked to update any conflicts of interest or provide details of secondary employment?	

Previous fraud control performance improvement initiatives

Can you think of any actions that have been taken in recent times (say, in the past year or so) to improve third party management systems, either at your workplace or for the organisation generally? Jot down any that you can think of.

Rating current performance

Thinking about what this attribute is seeking to achieve, and the perceptions about those outcomes that you have developed through your experiences, how would you rate this aspect of the fraud control environment?

Either: It is all news to me (I have never heard about it and see no signs that it exists) *or* it is clearly not working	Ok at best, but it's not very clear to me that it is working well	Seems quite good	Yes, it is clear to me that it is working very well
Score 1	Score 2	Score 3	Score 4

So that the group can discuss this, please make a few notes of the main reasons that have lead you to give this rating.

Your workshop facilitator will get the group to discuss the various ratings that people came up with, and why. This may bring things to your attention that you were not aware of, or help you to clarify your thinking.

After discussion, if you want to reassess the rating that you made, this is fine. The facilitator will seek to reach a group consensus on the rating, but this is not vital.

Determining Future Actions

For this attribute (only) of the fraud control framework, does your workplace, and/or the organisation, need to do something to improve the situation NOW? (Other things that you think may need to be done will be covered later under the other attributes.) *Please circle one.*

If 'yes', please make some notes below about:

- *what are the things that need to be done?*
- *who do you think should do it?*
- *by when?*

What?	Who?	When?

The group will come back to these later, to work out a shortlist of the top priority actions.

Notification systems

Just so you know

This is attribute eight (of ten) in your organisation's fraud control framework.

It is one of a number of elements that contribute to establishing a fraud control environment for the organisation.

This specific attribute would be working well if:

- **there is culture that supports staff reporting fraud and management acting on those reports**
- **there are well publicised options for staff to report fraud**
- **staff feel confident they will be protected from reprisal action**
- **your organisation can demonstrate the action it takes in response to reports of fraud**
- **there are polices, systems and procedures to support reporting with different reporting channels available**
- **your organisation provides feedback and follows up with internal reporters**
- **processes are in place to support upwards reporting**
- **actual and suspected frauds are reported to the CEO and audit and risk committee**
- **your organisation's fraud database is published on its website**
- **staff are clear on your organisation's policy and procedures on external reporting**
- **external reporting is made in accordance with legislation and policy**
- **your organisation takes a clear and consistent approach to external reporting.**

Signs of success?

Please consider your own views about the following points. People in different roles and at different levels may have different knowledge and different views about these matters – that is fine. Just say what you think, based on what you know.

Would most staff in your work area report suspect behaviours or actions that they knew about?	
Do most staff in your work area trust the organisation to deal genuinely with matters reported and to protect those who make genuine reports?	
Do most staff in your work area know about the systems and processes for reporting matters?	
Are the systems and processes for reporting matters simple and easy to use?	
Can matters be reported anonymously?	
Does your organisation publish its fraud database on the website?	

Table continues over the page.

Are most staff in your work area aware of the external reporting obligations that your organisation must meet?	
Are most staff aware of the purpose of external notification, and what happens when matters are reported to external bodies?	
Does your organisation have a policy on when reports will be made to external bodies?	
Does your organisation's annual report provide information to the community about instances of fraud reported to external bodies?	

Previous fraud control performance improvement initiatives

Can you think of any actions that have been taken in recent times (say, in the past year or so) to improve notification systems, either at your workplace or for the organisation generally? Jot down any that you can think of.

Rating current performance

Thinking about what this attribute is seeking to achieve, and the perceptions about those outcomes that you have developed through your experiences, how would you rate this aspect of the fraud control environment?

Either: It is all news to me (I have never heard about it and see no signs that it exists) *or* it is clearly not working	Ok at best, but it's not very clear to me that it is working well	Seems quite good	Yes, it is clear to me that it is working very well
Score 1	Score 2	Score 3	Score 4

So the group can discuss this, please make a few notes of the main reasons that have lead you to give this rating.

Your workshop facilitator will get the group to discuss the various ratings that people came up with, and why. This may bring things to your attention that you were not aware of, or help you to clarify your thinking.

After discussion, if you want to reassess the rating that you made, this is fine.

The facilitator will seek to reach a group consensus on the rating, but this is not vital.

Determining Future Actions

For this attribute (only) of the fraud control framework, does your workplace, and/or the organisation, need to do something to improve the situation NOW? (Other things that you think may need to be done will be covered later under the other attributes.) *Please circle one.*

If 'yes', please make some notes below about:

- *what are the things that need to be done?*
- *who do you think should do it?*
- *by when?*

What?	Who?	When?

The group will come back to these later, to work out a shortlist of the top priority actions.

Detection systems

Just so you know
This is attribute nine (of ten) in your organisation's fraud control framework.

It is one of a number of elements that contribute to establishing a fraud control environment for the organisation.

This specific attribute would be working well if:

- **your organisation has well documented risk-based internal controls and undertakes routine checks of activities, processes, controls and transactions**
- **available data is monitored and reviewed to ensure irregularities and warning signs are picked up early**
- **early warning signs are acted on quickly and red flag behaviour recognised.**
- **your organisation has a risk based internal audit program that evaluates the potential for fraud and how fraud risk is managed**
- **internal audit recommendations are assigned to individuals with timeframes for response.**

Signs of success?
Please consider your own views about the following points. People in different roles and at different levels may have different knowledge and different views about these matters – that is fine. Just say what you think, based on what you know.

Are routine checks of activities, processes, controls and transactions undertaken at your work area as part of local management and review?	
Are any data mining tools used locally?	
Would most staff in your work area be able to identify 'red flag' behaviour associated with fraudulent activity?	
Has your work area been reviewed by internal audit within the past three years?	

Previous fraud control performance improvement initiatives

Can you think of any actions that have been taken in recent times (say, in the past year or so) to improve detection systems, either at your workplace or for the organisation generally? Jot down any that you can think of.

Rating current performance

Thinking about what this attribute is seeking to achieve, and the perceptions about those outcomes that you have developed through your experiences, how would you rate this aspect of the fraud control environment?

Either: It is all news to me (I have never heard about it and see no signs that it exists) *or* it is clearly not working	Ok at best, but it's not very clear to me that it is working well	Seems quite good	Yes, it is clear to me that it is working very well
Score 1	Score 2	Score 3	Score 4

So that the group can discuss this, please make a few notes of the main reasons that have lead you to give this rating.

Your workshop facilitator will get the group to discuss the various ratings that people came up with, and why. This may bring things to your attention that you were not aware of, or help you to clarify your thinking.

After discussion, if you want to reassess the rating that you made, this is fine.

The facilitator will seek to reach a group consensus on the rating, but this is not vital.

Determining Future Actions

For this attribute (only) of the fraud control framework, does your workplace, and/or the organisation, need to do something to improve the situation NOW? (Other things that you think may need to be done will be covered later under the other attributes.) *Please circle one.*

If 'yes', please make some notes below about:

- *what are the things that need to be done?*
- *who do you think should do it?*
- *by when?*

What?	Who?	When?

The group will come back to these later, to work out a shortlist of the top priority actions.

Investigation systems

Just so you know

This is attribute ten (of ten) in your organisation's fraud control framework.

It is one of a number of elements that contribute to establishing a fraud control environment for the organisation.

This specific attribute would be working well if:

- **your organisation has clear documented investigations procedures**
- **staff are confident that reports of fraud will be investigated promptly and to the highest standards**
- **investigations are independent**
- **sufficient resources are allocated to investigations, including budget.**
- **investigations are conducted by qualified and experienced staff with recognised qualifications and appropriate experience**
- **your organisation has documented decision making processes**
- **staff understand fraud will not be tolerated and the perpetrators will face disciplinary action**
- **your organisation has a commitment to taking action against the perpetrators of fraud**
- **your organisations applies sanctions consistently.**

Signs of success?

Please consider your own views about the following points. People in different roles and at different levels may have different knowledge and different views about these matters – that is fine. Just say what you think, based on what you know.

Do most staff in your work area have confidence that any fraud investigations would be undertaken to required standards and by appropriately qualified staff?	
Do most staff in your work area have confidence that identified perpetrators of fraud will be successfully prosecuted based on sound investigative work?	
Is it clear to most staff that fraud is a crime and perpetrators will be prosecuted?	
Do staff refer to examples where they feel that people were 'let off' lightly?	

Table continues over the page.

In situations where substantive fraud is not established but breaches of acceptable ethical behaviour are proven, are the disciplinary standards and consequences clear to staff?	
Do most staff think that the organisation's conduct and disciplinary policies are clear, not contradictory and applied consistently?	

Previous fraud control performance improvement initiatives

Can you think of any actions that have been taken in recent times (say, in the past year or so) to improve investigation systems, either at your workplace or for the organisation generally? Jot down any that you can think of.

Rating current performance

Thinking about what this attribute is seeking to achieve, and the perceptions about those outcomes that you have developed through your experiences, how would you rate this aspect of the fraud control environment?

Either: It is all news to me (I have never heard about it and see no signs that it exists) *or* it is clearly not working	Ok at best, but it's not very clear to me that it is working well	Seems quite good	Yes, it is clear to me that it is working very well
Score 1	Score 2	Score 3	Score 4

So that the group can discuss this, please make a few notes of the main reasons that have lead you to give this rating.

Your workshop facilitator will get the group to discuss the various ratings that people came up with, and why. This may bring things to your attention that you were not aware of, or help you to clarify your thinking.

After discussion, if you want to reassess the rating that you made, this is fine.

The facilitator will seek to reach a group consensus on the rating, but this is not vital.

Determining Future Actions

For this attribute (only) of the fraud control framework, does your workplace, and/or the organisation, need to do something to improve the situation NOW? (Other things that you think may need to be done will be covered later under the other attributes.) *Please circle one.*

If 'yes', please make some notes below about:

- *what are the things that need to be done?*
- *who do you think should do it?*
- *by when?*

What?	Who?	When?

The group will come back to these later, to work out a shortlist of the top priority actions.

Facilitator's Workshop Summary

Final Assessment

Actions and Priorities

Over the course of this workshop, a series of actions have been discussed.

Those actions should be consolidated into one place to be reviewed by the group.

A final brief discussion should then be held to determine whether there are some actions that are more important than others, duplications, overlaps, or simplifications that can be made.

The group will also need to determine how many actions are practical now (is it practical, for example, to have more than five or six key actions?)

For each final action, responsibility for implementation should be noted, together with a timetable.

Final Actions for Implementation

List below the final actions to be taken, together with responsibility for that action and the associated timetable:

Action	Priority	Responsibility	Timetable

This completes the Fraud Control Improvement Workshop for this work area.

Actions flowing from this workshop will be monitored by the audit and risk committee.

Resource five: Sample fraud control policy

1. Introduction

Use the introduction to define fraud and to make it clear that the policy applies to all staff, including permanent, temporary, part time, contractors and consultants.

The introduction (or background section) should also explain the context of the fraud control policy and how it is part of a wider ethical framework.

2. Fraud Control Framework

Explanation of the fraud control framework – you can use the graphic from the Audit Office guidance to explain the framework, that is, ten key attributes which sit within the themes of prevention, detection and response.

Attribute one: Leadership

Use this attribute as an opportunity to state the organisation's commitment to managing fraud – endorsed by the CEO.

Link to other relevant articles, presentations and so on, by the CEO which demonstrates the organisation's commitment to managing fraud.

Link to management and corporate plans setting out responsibilities of senior managers for fraud control.

Attribute two: Ethical framework

Set out a high level summary of organisation core values and link to other ethical behaviour policies such as the code of conduct, gifts and benefits, secondary employment and conflicts of interest.

Attribute three: Responsibility structures

Identify specific responsibilities within the organisation, for example:

- senior managers
- fraud prevention manager
- internal audit
- external audit
- audit and risk committee
- fraud control committee
- all staff.

Attribute four: Fraud control policy*

High level commitment to managing fraud.
Alignment with Australian standards.

* this document is the fraud control policy.

Attribute five: Prevention systems

Set out the organisation's commitment to regular fraud risk assessments.

Provide a link to fraud database (which should be published on the website) and explain how the data will be used.

Explanation of pre-employment screening program and why this is important.

Link to IT security strategy.

Attribute six: Fraud awareness

Summary of awareness raising program – internal and external with relevant links. Brief overview of why the awareness raising program is important.

State the organisation's commitment to providing regular training for staff.

Attribute seven: Third party management systems

Include an explanation of why robust third party management systems are important and a brief summary of the type of work that is delivered by third parties in your organisation.

Set out the requirement for third party due diligence and give some high level examples of internal controls.

Provide a summary of the ways that third parties can report allegations of fraud.

Explain the education and training program for key staff.

Attribute eight: Notification systems

Mechanisms for reporting – different channels that are available and option to report anonymously.

Management commitment to act on reports of fraud.

Make a commitment to protecting reporters from reprisals and make it clear that confidentiality will be maintained.

Links to other reporting policies, for example, public interest disclosures.

Set out the organisation's policy on when reports will be made to external bodies.

Attribute nine: Detection systems

Provide a high level summary of the internal audit program – why particular areas will be reviewed and what internal audit will focus on.

Give some examples of internal controls.

Attribute ten: Investigation systems

Explain the standards required of investigations and investigators – link to investigation policies and procedures.

Explain the consequences for staff committing fraud and link to the organisation's disciplinary procedures. Set out the commitment to take action against perpetrators of fraud.

Set out the organisation's commitment to recovery action.

Resource six: Procurement checklist

Mitigating procurement fraud

Effective entity level controls should include:

- ❑ acknowledge the risk of procurement fraud on your risk register, and assign a risk owner who has overall responsibility in the organisation
- ❑ train staff in the awareness and prevention of fraud and how to identify procurement fraud
- ❑ ensure procurement policies and processes are documented, readily available to all staff, followed and enforced and regularly reviewed
- ❑ consistently enforce segregation of duties
- ❑ ensure procurement contracts stipulate sub-contractors must be agreed to before they are engaged
- ❑ proactively assess prevention of procurement fraud. Undertake proactive data set matches and analyse available data from systems. Utilise system generated exception reporting
- ❑ engage internal audit and ensure they include procurement testing in their annual audit plan
- ❑ establish escalation procedures to inform the relevant level of management on potential or actual fraud
- ❑ review major vendor relationships with senior staff and decision makers
- ❑ ensure adequate IT security controls are in place and ensure access to systems is appropriate
- ❑ establish appropriate audit trails for vendor management and payment tolerances.

Procurement process controls and tests

Type of Fraud	Description	Red Flag	Preventative controls	Detective procedures
Conflicts of interest	• Misusing position to award contracts to firms in return for personal gain (money, family employment, or other gratuities) • Conflicts can be actual, perceived or potential	• Lifestyle changes • Refusal to change vendors • Failure to enable proper bidding procedures • Continuous use of same vendor • Significant increase in pricing • Increase in product complaints • Poor cash management practices (payment outside of regular terms based on industry norms) • Favouring a bidder or supplier in a prejudicial manner	• Conflict of interest/related party registers • Gift registers • Consistently implemented procurement policies • Complaints registers • Internal reporter policies and procedures • Fraud policies and training • Education and awareness programs • Code of conduct	• Review relevant registers / complaints / notifications / internal audit investigations • Confirm action taken is appropriate in response to complaints etc. • Confirm processes are consistently applied • CAAT[3] ASIC related party check • Data analytic tool – related parties = fields in vendor master file • Data analytic tool – payment outside of terms • Check employee bank account details against vendor bank account details
Phantom vendor	• Employee establishes a fictitious vendor and submits false invoices for payment (or invoice may not exist to support payment)	• False / missing / incomplete / photocopied supporting documentation • Master file change authorisations are for short terms / or are regularly repeated • Duplicate payments / unusual spending patterns / slight variations of vendor names / multiple invoices paid on the same date / employee-vendor matching/out of sequence invoices	• Access to modify the Vendor Master File is restricted • Changes made are not made to the Vendor Master File without approval or support • Periodic review of the Vendor Master File and edits made to the Vendor Master File • Proper segregation of duties • System generated exception reporting of master file changes (reviewed and	• Data analytic tool - testing of unusual Master file changes / unusual transactions / expired contracts • Data analytic tool - matching of payroll/ employee address / telephone number fields / contact details • Transaction testing to supporting documentation • Analyse data (business trends / comparative data • Analyse transactions (top vendors by

[3] CAAT – Computer Assisted Audit Techniques

Procurement process controls and tests

Type of Fraud	Description	Red Flag	Preventative controls	Detective procedures
		• Use of expired contracts / inactive vendors • Contract not in place • Failure to complete match of invoices to receiving and order documentation • Vendors with PO box as sole address • Cheques set aside for pick-up • Invoices received after payment is made • Employee details match vendor details • Lack of review of access controls commensurate to duties	actioned by senior users) • System generated exception reporting of unmatched items (reviewed and actioned by senior users) • Restriction of master file input to approved field parameters • Ensure staff access to systems and processes is appropriate and kept updated • Follow government procurement standards and use standard contract templates	payment type / quality, issues / shipping irregularities. • CAAT list suppliers' and employees' details if supplier address = employee address • CAAT employee bank account record = vendor bank account record • CAAT vendors missing ABN / vendors with invalid ABN • Profile vendor transactions for partial payments and audit • Review credit notes
Split purchase orders/split orders		• Amounts raised are just below delegation levels to override authorisation requirements • Invalid GST number • Out of hours transactions • Low initial bids followed by excessive change requests	• Proper segregation controls • Review of system output / exception reporting by senior users • System generated exception reporting (reviewed by senior users) • Variation limits for costs on contracts and projects are stipulated and deviations are investigated	• Data analytic tool - test for repeat amounts / POs with the same or out of sequence numbers / high volume authorisations from single users / contract variations • Review aged POs to ensure payment is not made more than once.

Procurement process controls and tests

Type of Fraud	Description	Red Flag	Preventative controls	Detective procedures
Kickbacks/ bribery	• Misusing position to award contracts to firms in return for personal gain (money, family employment, or other gratuities • Often facilitated through accounts payable. Supplier submits an invoice for services that never occurred. • Invoice submitted is inflated by the amount of the kickback sent to the conspiring employee. • Making corrupt payments to foreign officials for the purpose of obtaining or keeping business	• Large gifts and entertainment expenses • Unusual increases in vendor spending • Tips and complaints • Inflated charges • Restricted list of eligible suppliers • Non-genuine competition (suppliers with common ownership data) • Lifestyle changes of procurement staff • Refusal to change vendors • Failure to enable bidding procedures • Significant increase in pricing • Increase in product complaints • High commission payments	• Appropriate policies and procedures, properly implemented and enforced. • Proper investigation of complaints (internal and external) • Clear authorisation / sign-off levels for: - initiation of tender processes - new contracts - contract renewals and extensions • Education and awareness campaign • Keep register of organisations known to act fraudulently/ • inappropriately • Gifts and benefits policy	• Review of gift registers • Analysis of spending patterns with vendors • Review of supporting documentation of tender processes • Review of goods returned patterns • CAAT list all invoices if invoice amount > supplier credit limit

Procurement process controls and tests

Type of Fraud	Description	Red Flag	Preventative controls	Detective procedures
Duplicate payments	• Duplicate payments made to a vendor without services rendered to justify the second payment. This fraud is normally committed by a vendor with collusion with an employee.	• Multiple duplicate payments of the same or similar amounts to a vendor and/or for the same invoice	• Matching of payments to original, authorised payment orders and goods received notifications	• Data analytic tool - test for payments and invoices for same amount / invoice details / duplicate dates • Trace payment detail to unique supporting documentation • Test for three way matching exception reports • CAAT Duplicate payments • CAAT duplicate invoices same vendor: same invoice number and amount • CAAT duplicate vendors by bank account
Bid rigging	• Collusive price-fixing behaviour by which firms coordinate their bids on procurement or project contracts, including arrangement of bidding process to guarantee selection of vendor	• Improperly secured bids • Bid suppression – vendors fail to participate or withdraw from process • Bid rotation amongst suppliers • Rebids to selected vendors • Excessive use of suppliers without business justification • Excessive subcontracting of successful tenders • Supply of faulty / inferior materials • Excessive control over selection process • Inflated pricing • Bids not awarded to lowest bidder without adequate explanation	• Documented policy and procedures for tender / bid / quote processes rigorously enforced and oversighted by persons independent of procurement process • Segregation of duties between bid processes and procurement function • Investigation of complaints	• Review controls around the bidding process for poor documentation / absence of appropriate competition / manipulation of evaluation criteria • Review handling of complaints