Fraud Management Toolkit

NOVEMBER 2020

Office of the Independent Commissioner Against Corruption NT

"As public servants we have an extraordinary opportunity to make a real contribution to our communities. The community and the government rightly expect us to undertake our work on their behalf conscientiously and professionally. When something goes wrong we need to act in a timely and decisive manner. This is crucial to maintain the trust of the government and the community in our ability to manage ourselves. We must address poor or risky behaviour and misconduct promptly when it is identified."

The Australian Public Service Commission
– A culture of integrity

This guide has been designed to help public sector managers think about integrity risks in their workplaces, and provide some guidance about steps that they can take to help their agency maintain high levels of integrity.

Contents

Defining fraud

Fraud is not defined in the Northern Territory (NT) *Criminal Code*. The following is extracted from NT *Treasurer's Direction — Fraud Control*. That Direction defines fraud as:

- Obtaining (or attempting to obtain) a financial benefit, or causing (or attempting to cause) a financial loss, by deception.
- Obtaining a financial benefit includes obtaining for oneself, another person, or a third party.
- Fraud requires more than carelessness, accident, or error – in these cases, an incident may be non-compliance rather than fraud.

The Australian Government's *Government Fraud Control Framework* 2017 lists the behaviour that is included in the definition of fraud, noting that the list is not exhaustive:

- theft
- accounting fraud (e.g. false invoices, misappropriation)
- misuse of government credit cards
- unlawful use of, or unlawful obtaining of, property, equipment, material or services
- causing a loss, or avoiding and/or creating a liability
- providing false or misleading information to the government, or failing to provide information when there is an obligation to do so
- misuse of government assets, equipment or facilities
- cartel conduct
- making, or using, false, forged or falsified documents, and/or
- wrongfully using government information or intellectual property.

Fraud requires intent. It requires more than carelessness, accident or error. When intent cannot be shown, an incident may be non-compliance rather than fraud.

A benefit is not restricted to a material benefit, and may be tangible or intangible, including information. A benefit may also be obtained by a third party.

Internal fraud is where fraud against a public body is committed by its public officer or contractors.

External fraud is where fraud comes from outside the public body from external parties such as clients, service providers, members of the public or organised crime groups.

Public bodies should be alert to the risk of **complex fraud** involving collusion between their public officers and external parties. Complex fraud can include instances when a public officer or group of public officers:

- are targeted and succumb to exploitation by external parties (bribery, extortion, grooming for favours or promises), or
- initiate the misconduct (including through external parties infiltrating the public body).

Fraud can include corrupt conduct where the corrupt conduct results in a party obtaining a benefit from, or causing a loss to, the government. An example of this is collusion between a public officer and a contractor. Some forms of corrupt conduct, such as soliciting for bribes or secret commissions, may not cause a direct financial loss to government. However they may distort the market for fair provision of services or inflate prices, and may damage the NT's reputation and the public's trust in government. Not all corrupt conduct falls under the definition of fraud.

By contrast, **trivial fraud** (less significant) refers to matters that may technically meet the definition of fraud but are not serious enough to warrant any formal action beyond a managerial response. However, it is important for agencies to be mindful that incidents of 'trivial fraud' could be indicators of more systemic problems or vulnerabilities.

Corrupt conduct

The *Independent Commissioner Against Corruption Act 2017* (the ICAC Act) defines corrupt conduct as conduct engaged in by a public officer (whether or not the identity of the public officer is known) or by a public body:

1. that constitutes an offence, whether in the Territory or elsewhere, for which the maximum penalty is imprisonment for a term of at least two (2) years (with or without a fine); and
2. is connected to public affairs; and
3. the conduct constitutes reasonable grounds for dismissing or terminating the services of a public officer; and
4. the conduct is connected to public affairs, and involves any of the following: dishonesty; failure to manage adequately an actual or perceived conflict of interest; a breach of public trust; the illegal, unauthorised or otherwise inappropriate performance of official functions; inappropriate conduct in relation to official information; an adverse effect on the honest, impartial or effective performance of official functions by any public officer or public body or group of public officers or bodies.

Conduct is corrupt conduct if it is engaged in by a public body, minister, MLA or local councillor if the conduct is connected to public affairs and involves a serious breach of trust.

Conduct is corrupt conduct if it is engaged in by a person (whether or not a public officer or public body) that could impair public confidence in public administration, and that involves any of the following:

1. collusive tendering;
2. intentionally or recklessly providing false or misleading information in relation to an application for a licence, permit or other authority under legislation designed to:
   a) promote or protect health and safety, public health, the amenity of an area;
   b) facilitate the management and commercial exploitation of resources;
3. misappropriating or misusing public resources, or assisting in or dishonestly benefitting from the misappropriation or misuse of public resources;
4. dishonestly obtaining or retaining employment or appointment as a public officer.

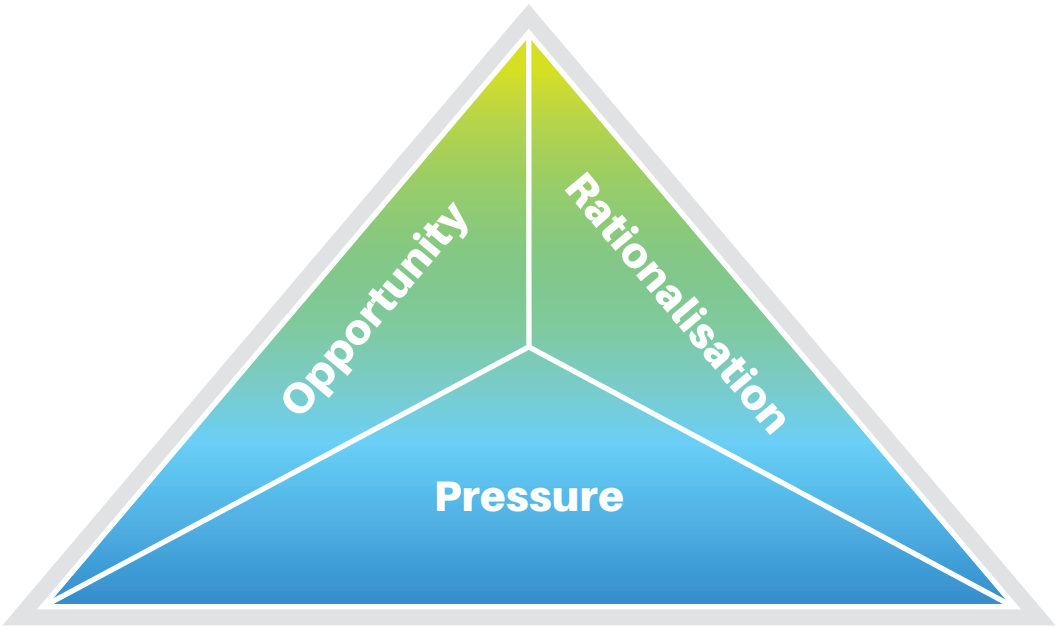
Conduct is corrupt conduct if it is engaged in by a person (whether or not a public officer or public body) that constitutes:

1. an offence against Part IV, Divisions 1 to 5 of the Criminal Code (offences against the administration of law and justice and against public authority); or
2. an offence against sections 118 or 119 of the Criminal Code (false statements under oath or solemn declaration; false declarations and statements); or
3. an offence adversely affecting, directly or indirectly, the honest, impartial or effective performance of official functions by any public officer or public body or group of public officers or public bodies, and that is prescribed by regulation.

Examples include but are not limited to:

1. intervening in a procurement process to ensure someone you know is awarded a contract;
2. as a selection panel member for public officer position, failing to disclose that you are in a relationship with one of the applicants;
3. using discretionary powers that form part of your official duties to personally benefit yourself or others; and/or
4. submitting false invoices for payment to you personally or to someone known to you.

The fraud triangle



Donald Cressey[1] created the fraud triangle, identifying three factors that must be present at the same time in order for an ordinary person to commit fraud. Those three factors are pressure, opportunity and rationalisation.

Pressure is the first factor. It is what motivates the fraud in the first place.

The person has some financial problem they are unable to resolve by legitimate means so they begin to consider an illegal act. A financial problem can be personal or professional.

Opportunity is the second factor and it defines the method by which fraud can be committed.

The person must see some way to use or abuse their position of trust to solve the financial problem with a low perceived risk of being caught.

Rationalisation is the third factor.

The vast majority of people who commit fraud are first-time offenders with no criminal history; they don't see themselves as criminal. Rather, they see themselves as ordinary, honest people who are caught in a bad set of circumstances and thus rationalise their illegal activity.

[1]Cressey, DR (1973) *Other People's Money,* Montclair; Paterson Smith.

Identifying risk

Public sector fraud: identifying the risk areas

The following areas were identified by Deloitte (2008[2]) as most commonly at risk in the public sector. The findings arose from audits done throughout the preceding year.

Failure to adhere to procurement procedure

This may involve bid rigging or avoiding formal tendering requirements so as to favour a particular supplier. This may be done in return for a direct financial reward, or, as in a case that was investigated, because the purchasing manager had a personal preference for a particular technology type and avoided putting significant expenditure requests through a formal tender process. This was despite continued complaints from staff at the organisation because the chosen technology failed to meet their requirements.

Abuse of expense policies

Employees may take advantage of loosely worded policies, or of their ability to authorise their own expenses. In one case, a senior employee had attended courses overseas, but had stayed on at the location after the course had ended, and claimed the hotel and other costs back from his employer. The same individual had made claims for mileage and for train travel to identical locations on the same dates.

Collusion with external suppliers or creation of fictitious suppliers

Where senior personnel are able to set up and authorise payments to suppliers, there is a risk that the organisation can end up paying for services that it has never received, or paying too much. An example includes significant sums paid to the overseas-based related party of a senior manager, despite the fact that similar products were available at cheaper prices locally. One way to identify such related party frauds can be to compare the bank account details of suppliers to those of employees and see if there are any matches.

Misuse of public assets for personal gain

In two cases, instances of employees running private businesses were uncovered, whilst being employed by, and using the assets of a semi-state body. In one of these, there was an additional risk to the body because the employee was engaged in illegally copying software.

Misreporting of budgets to obtain funding

Where funding is under pressure, organisations may be tempted to report results which will maximise their funding, rather than results that properly record their expenditure. The impact of this is that scarce funding may be incorrectly allocated and, as outlined by the Comptroller and Auditor General: "Good financial management demands that public funds should only be disbursed as needed. Allocating scarce resources to projects before they are clearly in a position to proceed may unnecessarily delay other projects of equal merit due to a perceived lack of available funding."

Overtime or contractor abuse

Employees or contractors can take advantage of weak controls to overcharge for work done. Some simple data analytics tools can help organisations to identify potential over-claims which can then be followed up for investigation with any loopholes being closed off by improved policies and controls.

[2]*Public sector fraud: identifying the risk areas.*

Fraud reduction plans

Public sector bodies can do a lot to reduce the risks of fraud by adopting a clear fraud reduction plan.

Ten key issues to consider when putting in place a fraud reduction plan in the public sector are:

1

Tone at the top

Senior management must send out the message that fraud in any form is not going to be tolerated, and lead by example.

2

Clearly written policies and procedures

These should spell out carefully and simply what is not allowed and the consequences of violating the rules. In addition, management should consider testing the attitude of staff to ethics by means of regular surveys.

3

Allocate responsibility for fraud risk management

To avoid the risk that responsibility falls between managers, the organisation should have a clear fraud risk champion, who is known to all employees.

4

Training

A written policy needs to be supplemented by training to ensure that there are no grey areas in regard to acceptable conduct. Online or face-to-face training enables employees to understand how the policy applies in real life situations.

5

Whistle-blowing

Encourage employees to highlight potential problems by implementing a mechanism that provides a confidential method to report concerns. Nearly half of all fraud is uncovered by tip-off.

6

Implement strong anti-fraud controls

This is just as essential in the public sector as it is for any other organisation. In particular segregation of duties should never be compromised. It is also important to ensure that these controls apply to peripheral areas – for example, cafeterias, car parks or other non-core activities.

7

Fraud risk management

A regular review of fraud risks should take place to identify where the organisation faces the greatest risk of loss. Control and audit resources can then be devoted to the areas where they will have the greatest impact.

8

Enforcement as deterrent

There can be a fear of the negative impact of reported fraud on an organisation, but simply letting the perpetrator resign does little to discourage future wrongdoing by others.

9

Paying attention to small transgressions

Since fraud generally starts small and can grow over time, addressing even the smallest transgressions can be instrumental in preventing future scandals. It also sends out the message that fraud is not acceptable.

10

Prevention first

Once fraud has been committed and the money spent, it is difficult to recoup the losses. It is far better to keep theft from happening in the first place.

Managing risks in the workplace

Bringing people into your workplace

The first few weeks after an employee has joined an agency are a unique opportunity to make sure that they understand how the agency works and what is expected of them, and to establish good working habits.

Each manager has a key role to play that complements the normal agency induction process. Managers have the ability to look at new starters as individuals, as people with unique backgrounds, skills and experience. New starters may bring with them a different set of professional values that are not consistent with Northern Territory Public Sector (NTPS) principles. They may not fully understand the conventions that are part of being a professional public servant.

1.1 Post-recruitment risks

- the new recruit is not properly integrated into the agency and its cultural norms during the induction and probation processes
- the new recruit is corruptly influenced to make decisions in favour of a third party
- the new recruit is linked to a group that is seeking to infiltrate the agency.

1.2 Mitigating the risks

The time that you put into a new starter is an investment in their future behaviour and performance. It may be helpful to ask yourself:

- does the employee understand how the NTPS Principles and Code of Conduct apply to them?
- is there anything special about the employee's background or experience that raises particular issues of concern? For example, were they previously employed by a lobby or special interest group that might raise questions of conflict of interest?
- has the employee been briefed about the acceptable use of information and communications systems and equipment?
- is the employee aware of any office security requirements?
- does the employee know how and where they can report any threat to the integrity of your agency?
- have you discussed:
  - how the Principles and Code apply—including behaviour outside the workplace?
  - whether they have any conflicts of interest in the performance of their duties?
  - the need to declare any gifts or benefits they receive as part of their employment?

Probation is the primary tool to mitigate against integrity risks where the new recruit is commencing with the NTPS.

What else a new person needs to know:

- roles and responsibilities
- privacy and non-disclosure legislation
- conflict of interest policy and management
- how to report risks or threats to integrity
- reporting requirements under the *ICAC Act*
- agency policy on outside employment.

Tools and resources

- Using conditions of engagement to mitigate risks
- OCPE training programs.

1.3 Changed personal circumstances

Changes in an employee's circumstances may increase their vulnerability to integrity risks.

All employees experience changes in their personal, financial and employment circumstances in the course of their career. Some of these may give rise to integrity risks, making the employee more vulnerable to temptation, blackmail, targeted advances by malicious insiders or external threats.

A relationship breakdown may trigger both emotional and financial stress which could make the employee look for opportunities for financial gain. Changed work circumstances such as a loss of status, demotion or lack of promotion opportunities may cause bitterness and resentment in an employee who then seeks revenge.

One-off changes to normal patterns of behaviour, for example arriving late to work for a couple of days in a row, would not normally be a matter for concern. Managers should be on the lookout for repeated and sustained behavioural changes. The section on *Identifying other integrity risks* gives an idea of the types of behaviour to look out for that might indicate the employee poses a risk.

1.4 Organisational change

Organisational change can cause stress in employees' work lives and affect morale.

Employees who report that their agency managed change poorly have considerably lower engagement levels than other agencies. Poorly managed change has a larger impact on engagement than any other factor.

Decreased levels of employee engagement have the potential to become an integrity risk and should be properly managed.

Managers should focus on maintaining open and honest two-way communication during periods of change, and help employees who display signs of stress, agitation or resentment.

1.5 Ongoing suitability assessment

Agencies are required to monitor the suitability of employees on an ongoing basis. Any concerning behaviour in individuals holding security clearances must be reported, as well as any significant changes in personal circumstances, including changes reported to the agency by a third party.

There is a need to change focus from point-in-time suitability assessments to continuous monitoring and assessments of each person's ongoing suitability.

Employee vetting is an effective means of ensuring a basic level of trust only at a particular point in time. As employees' circumstances, attitudes, behaviour and motivations will change over time, and vetting 'aftercare' is vital.

The ongoing suitability of employees must be monitored over time for changes to their role or their personal circumstances and behaviour. Responsibility needs to be clearly allocated to the appropriate manager and understood by the employee.[3]

[3]Colwill, C. (2009) 'Human factors in information security: The insider threat—Who can you trust these days?' in *Information Security Technical Report*, November 2009.

1.6 Conflicts of interest

The management of real and potential conflicts of interest is a central element of establishing a strong integrity culture. Managers and employees need to think carefully about how actual or perceived conflicts of interest can affect their actions and the reputation of their agency.

The principle is simple: NTPS employees should work to support the public interest within the framework of the law and of Northern Territory Government policy. Their actions and decisions should not be affected by their own private interests.

Interests that can affect, or be seen to affect, behaviour are broad in character. They include financial interests, but also things like family relationships, social relationships, or membership of a political party.

The NTPS Code of Conduct requires employees to disclose any conflict of interest and take reasonable steps to manage that conflict, but it is often the case that people don't recognise that they have a conflict.

Managers can help their staff by creating a culture in their workplace that encourages disclosure and where discussion about potential conflicts of interest is part of the way business is done in that agency. They should also ensure that employees are aware of their agency's policies on declaring and managing conflicts of interest, and on outside employment.

1.7 High risk roles

Some roles in agencies may present a higher risk of corruption.

High risk roles are not limited to frontline law enforcement positions or even customer service roles. Back office jobs, for example, can provide access to agency assets or information useful to criminal organisations. Managers need to think laterally to identify which positions may be at risk. These may include roles that have access to government funds or assets, significant financial delegations, or broad access to agency information and communications technology or sensitive information.

Managers need to think about appropriate mitigation and management strategies for potential risks. Formal risk assessments of high risk roles may be warranted.

1.8 Threats from organised crime

Public officers can be, and have been, targeted by organised crime entities to help them commit crimes. In some cases this can be the result of years of 'grooming' where criminal entities target and compromise an employee hoping that they will be useful in the future. Criminals may seek to corrupt public sector employees to gain access to public funds, sensitive information, protection and other services that help facilitate their criminal activities.

Employees may be at risk of coming into contact with organised crime groups unintentionally, such as through the purchase of recreational drugs, careless use of social media, or even gym membership.

The report of the former Australian Crime Commission on organised crime in Australia 2014-15 observed that:

> Social networking, the sharing of personal information on social media, and casual attitudes and the apparent growing tolerance of the general public toward 'recreational' or 'private' illicit drug-taking have been identified as having the potential to significantly increase the risk of corruption of younger public sector employees by bringing them into contact with organised crime groups.

The clear message here is while there are key roles and agencies within government that present risk, no area is immune from threat.

1.9 Out of hours conduct

1.9.1 Use of social media

Greater use of technology, including social media such Facebook, Twitter and Instagram, by employees may present a heightened integrity risk for agencies.

This can take a number of forms, such as:

- employees making inadvertent disclosures of sensitive information
- disaffected employees publishing information damaging to their employer or the government
- employees exposing themselves or their colleagues to identity theft.

Even relatively benign information about employees, such as where they work, who their colleagues are and the projects they are working on, can be used by people seeking to identify and compromise employees.

Managers have a role to ensure that their staff understand the responsibilities they have to use social media prudently.

1.9.2 Trips away and office parties

Risks to integrity may arise out of hours. Much-publicised risks occur during activities such as socialising on work trips away, and at social gatherings such as office Christmas parties. These are activities that may have a social component to them, and also pose real risks to the reputation of agencies.

Managers have a role to play here in reminding employees that the Code of Conduct can apply to work outside the usual workplace and outside normal working hours.

1.9.3 Mitigating the risks

Agencies are advised to develop social media policies that meet their needs and provide clear, simple tools for managers to explain requirements for employees.

Managers should consider reminding employees who are about to travel on business or to attend a work social gathering of the need to behave responsibly.

1.10 Privacy and trust

Very few employees engage in activities that would be regarded as a risk to integrity. The great majority of employees are honest and conscientious. Employees can be sensitive to and even resent the intrusion on their privacy of monitoring and recording of their activities.

Employees have a reasonable expectation that if there are issues that affect them, such as a conflict of interest, those issues will be addressed properly and proportionately. Employees will be discouraged from disclosing or reporting matters if they believe that they will not be dealt with fairly.

At the same time, agencies have a legitimate interest in putting in place policies and procedures that reflect the risks that they face. A balance needs to be found between the risk detection and monitoring needs of an agency and the reasonable expectations of employees.

Any monitoring system has the potential to reduce employee trust in the agency. If the process is carefully explained beforehand, and managed consistently, it is less likely to be considered unfair by employees or to damage trust. The monitoring process becomes just one more element of the day-to-day working conditions.

Source: adapted from https://www.apsc.gov.au/managing-risks-workplace

Recruitment fraud

Section 5C of the *Public Sector Employment and Management Act* defines the human resource management principle (HRM) as follows:

(1) The human resource management principle is that human resource management in the Public Sector must be directed towards promoting the following:

(a) employment based on merit

...

State of the Service Report, 2019-20, p 30

Merit-based recruitment is a fundamental element of Northern Territory Public Sector employment. Merit is about employing the best available person based on their work-related qualities and the requirements of the job.

What risk factors should I look out for?

The recruitment process includes identifying the job's requirements, attracting and screening applicants, offering employment to the best applicant and getting them on board. Each stage of this process has its own opportunities, but also its own risks.[4]

[4]Adapted from Victorian Public Service Commission (2015) *Integrity in Recruitment Guidance Note*.

Before advertising a vacancy

- Be sure that the job description or advertisement hasn't been written with a particular person in mind.
- The more broadly you advertise a position the broader the potential pool of applicants. This can be a positive by attracting applications from a broader pool of the community, but it can also attract applications from undesirable or even malicious applicants. What factors have affected your decision about where and how you have advertised?

Selecting panel members and decision-makers

- Have they had recent recruitment experience and merit selection and recruitment training?
- Do they understand their practical and legal obligations?
- Are there any conflicts of interest for the decision-maker or the selection panel? If so, how can these be addressed?
- Is the decision-maker independent and unbiased?

Assessing candidates

- Short cuts shouldn't be taken to recruit someone quickly at the expense of prudent checks.
- Don't assume that an applicant from an organisation with a good reputation will have a good employment history or a good character.
- Check the credentials and work history of an applicant carefully with third parties. This will be especially important if they will be working in a sensitive or strategically important area.
- Consider asking potential suitable candidates to undergo a criminal history check or obtain a national police clearance, particularly for highly sensitive positions or roles, prior to offering employment.
- Ask candidates to declare any potential conflict of interest relevant to the role for which they are applying. Suitability can be assessed against that and any conflicts managed accordingly.

Obtaining references

- Accurate referee reports are one way of avoiding the re-employment of people with bad work histories.
- Selection panels should remind referees of the need to give an honest assessment of work performance, attendance and behaviour.
- It is advisable in most cases to seek a reference from the applicant's current supervisor. It may also be a good idea to seek references from people who know the applicant but have not been nominated as a referee, letting the applicant know who you contact.
- Remember to check that the applicant's referee has accurately described their role or their relationship to the applicant.

Provision of false or misleading information prior to employment

Section 49 of the *Public Sector Employment and Management Act 1993* (PSEMA) deals with breaches of discipline, including where an employee has been dishonest when applying for NTPS employment.

Misconduct action can be taken if an employee is found to have:

- knowingly given false or misleading information, or
- wilfully withheld relevant information

about their background, qualifications, previous employment or other matters in connection with their engagement. This action can include termination of employment.

Dealing with historical Code of Conduct matters

An employee's previous misconduct may be relevant to their suitability for employment.

Agencies should consider asking specific questions about misconduct history in their job application processes, for example:

Sample misconduct history question

Are you currently being investigated for a suspected breach of the NTPS Code of Conduct? **Yes / No**

Have you ever been investigated for a suspected breach of the NTPS Code of Conduct or faced formal disciplinary or administrative action with any employer? **Yes / No**

If yes, what was the finding?.....

Date of breach determination/discipline action: ..... / ..... / .....

Sanction imposed (termination of employment, demotion etc.).....

A finding of misconduct will not necessarily exclude you from consideration for this vacancy.

Dealing with prior criminal history

A criminal conviction or pending charge does not necessarily exclude a person from NTPS employment. Nonetheless, a manager may be concerned that a conviction reflects on the person's fitness to perform particular duties, or affects the integrity and reputation of the NTPS or the safety of other employees.

Dealing with prior criminal histories will be affected by the 'spent conviction' scheme. It may be that after a specified period of time without reoffending a person convicted of a minor matter is able to present a 'clean slate'. In most cases a conviction that has been 'spent' does not need to be disclosed.

Refusing to employ a person on the basis of a criminal record that is not relevant to the proposed employment might be a basis for a complaint under discrimination and/or human rights legislation.

Mitigating recruitment risks

Applicants should be asked direct questions about their suitability for employment. Such questions might include their reasons for leaving a former employer, proof of qualifications and anything that could limit their ability to undertake a role, such as a relevant criminal record or a history of misconduct.

The recruitment process should explore any unexplained gaps in the applicant's employment history. There may be perfectly good reasons for such gaps. On the other hand, they might indicate that the applicant was dismissed by a previous employer or resigned while under investigation for misconduct.

Tools and resources

OCPE training programs.

Employees involved in assessing candidates in recruitment rounds should make sure that they understand the nature of the role and their responsibilities. Most agencies will have policies and advice about recruitment processes. Training is also often available to help managers identify and deal with issues in selection processes.

Pre-employment screening

Pre-employment screening, or background checking, is an integral part of managing recruitment risks.

Agencies should screen all new recruits to check their past employment and other background details. It's important that the claims made by applicants about their identity and achievements are accurate.

Offers of engagement, whether for ongoing or non-ongoing roles, should be clearly conditional on the applicant meeting specified conditions and requirements, including satisfactory completion of the probation period.

Tools and resources

- Using conditions of engagement to mitigate risks
- Template—integrity statement for letter of offer of engagement (see page 17)

Thoughtful and proportionate pre-employment screening for the preferred applicant before their engagement can have benefits. For example, if a pre-employment check reveals that a prospective employee will not meet the agency's citizenship requirements, the agency can decide not to engage that person.

Informing potential applicants in the job advertisement and information pack about pre-employment checks and conditions of engagement will help them decide whether or not to apply.

What should I look out for?

Pre-employment checks may include any of the following components:

- ✔ **identity verification**
  - gold standard identity verification—the 100 points system
- ✔ **eligibility**
  - Australian citizenship or valid visa with work rights
  - eligible and suitable to access Australian Government resources (see below for more information)
- ✔ **qualification checks**
  - verify mandatory qualifications by contacting the relevant institution rather than relying on documentation provided by the applicant
  - sight original academic records and other professional credentials
  - obtain evidence of any mandatory licences or registrations
- ✔ **previous employment checks**
  - verify employment history with previous employers, including roles and dates
  - undertake reference checks for previous work performance and conduct
  - review significant employment history gaps and reasons for those gaps
- ✔ **criminal record checks**
  - conduct national police checks
  - conduct working with vulnerable people checks if needed
- ✔ **agency-specific checks will depend on the circumstances, but might include**
  - character checks
  - credit checks
  - personal associations that could present a risk for the agency
  - any secondary employment that could present a conflict of interest with the role.

Mitigating pre-employment screening risks

Agencies may wish to consult the *Australian Standard AS 4811:2006–Employment Screening*.

Source: https://www.apsc.gov.au/managing-risks-when-recruiting

Template—integrity statement for letters of offer of engagement

The special nature of NTPS employment

Working in the NTPS is different from employment in other sectors. Public confidence in the NTPS is essential to the proper functioning of government. Public confidence and trust in the NTPS relies on its professionalism and adherence to high ethical standards.

Your engagement will be made in accordance with the *Public Sector Employment and Management Act 1993*. The Act also sets out the standards of behaviour required by the NTPS Principles and Code of Conduct—see Attachment A.

Your agency is bound by the *Information Act 2002*. A brief description of what this means for you is at Attachment B.

It is an offence to disclose information, sensitive material, to abuse public office and to engage in unauthorised access to, or modification of, data held in a Northern Territory Government computer or database.

Acknowledgement of professional behaviour

I acknowledge:

- the importance of acting fairly, impartially and courteously when dealing with members of the public, and in a way that is sensitive to their needs and backgrounds
- that it is essential to act with respect and courtesy in the workplace
- that the role of the NTPS is to serve the Government of the day regardless of which political party is in power
- that it is important for everyone I deal with to be able to trust that I will respect their privacy and confidences, and
- that members of the public are entitled to expect that public servants will act ethically.

I also acknowledge that:

- my employment is subject to the provisions of the *Public Sector Employment and Management Act 1993*, and that a failure to comply with any obligation of my employment may result in a finding that I have breached the Code of Conduct and may result in a sanction, including the termination of my employment
- I am obliged to uphold the reputation of the <*Agency*> and abide by the NTPS Principles and Code of Conduct.
- I am aware that the <*Agency*> is bound by the Australian Privacy Principles and I have been made aware of how my personal information may be used and to whom it may be disclosed.
- I have received <*agency to insert any other inclusions here. This may include key agency documents and useful information*>.
- I am aware that this offer of engagement may be cancelled before it takes effect for any reason, including if I supply false or misleading information relevant to my engagement.

Signature: ..... Date ..... / ..... / .....

Agency recruitment self-assessment

Claims of academic qualification	
	We require proof against claim by production of testamur.
	We require proof against claim by production of academic record.
	We require proof against claim by production of certified copy.
	We contact the institution to check past enrolment against claim.
	We require candidates to submit examples of their work.
	We require candidates to meet professional industry admission criteria.

References	
	We accept written references on face value.
	We do not accept written references.
	We ask candidates to nominate referees who are then contacted by the recruitment panel.
	We require that at least one referee is a former supervisor.
	We ask candidates whether any of their referees are relatives and/or friends.

Suitability for position	
	We ask candidates whether they have friends and/or family working in our public body.
	We ask candidates whether they have conflicts of interest.
	We ask candidates whether they have a criminal conviction that would affect their ability to undertake the duties of the position.
	We ask candidates to declare that all information they have provided is true and correct in every particular.
	We ask candidates to declare whether they have been subject to investigation for code of conduct breaches or disciplinary matters.

Special Measures claims	
	We ask candidates to support their claims of Special Measures qualification.
	We ask candidates for proof of their Special Measures qualification claim.
	We seek to verify Special Measures qualification claims with former employers.
	We accept Special Measures qualification claims on face value.

Selection panels	
	We require all members to have undertaken OCPE recruitment training.
	We provide internal training for selection panels.
	We have written policies applicable to selection panels.
	We rely on the common sense of our selection panels.
	We have a conflict of interest management process for selection panels.

Managing risks associated with former employees

Agencies should develop procedures to highlight any conflicts that may arise when an employee intends to separate from the NTPS.

What are the risks?

Former employees might reach back to the agency to seek inside information, favours or assistance from previous work colleagues. A post-employment job or contract may be given to them in exchange for an advantage they have provided while still a public officer. They may inappropriately disclose information.

Risks can also arise when separating employees are not properly removed from access to IT systems or have not returned equipment such as passes or laptop computers. Other risks arise from the increasing numbers of employees who bring their own IT equipment, such as laptop computers and USB drives, into the workplace, or undertake work from home.

Risks relating to post-separation employment include former employees who might:

- use their position to influence decisions and advice in favour of the prospective new employer while still employed
- reveal confidential Northern Territory Government information to their new employer or provide other information that might give the new employer a business advantage
- use their knowledge of the NTPS to lobby for their new employer in dealing with the Northern Territory Government.

Mitigating the risks

Steps can be taken to mitigate any conflict of interest while the individual who has decided to leave is still employed in the NTPS, including:

- re-allocation of the employee's duties
- temporary movement to a different work area
- taking leave until the new appointment commences.

Having sound exit protocols in place, including exit interviews and ensuring employees know the rules prohibiting the release of certain information, can help reduce the risk.

Sample employee exit checklist

Exit interview

- Conduct exit interview and seek feedback on matters relating to integrity in the agency
- Obtain forwarding address

Collect Northern Territory Government property

- Identity pass and name tag
- Keys – building, office and filing cabinets
- Mobile phone and charger
- Computer and devices – laptop/iPad/tablet
- IT equipment – software, remote access device, flash drives and storage devices
- Documents – hard copy files, electronic files, books, business cards
- Passwords/codes – desktop computer, laptop, phone, network and other IT systems
- Corporate credit card
- Vehicle, keys, fuel card and toll card
- Cab charges

Cancel access

- Building access cancelled
- Carpark access cancelled
- Computer login and network access disconnected
- Other database or system access cancelled
- Email address cancelled
- Voicemail cancelled
- Remote access cancelled
- Corporate memberships cancelled or reallocated

Adapted from: https://www.apsc.gov.au/managing-risks-do-former-employees

Identifying other integrity risks

Risks to integrity arise in various ways. Integrity breaches are more likely to occur where there is a poor workplace culture; substandard administrative and risk management processes; unclear policies and procedures; ignorance of legal and ethical obligations; and/or failures in accountability systems.

But integrity is not just about protecting our agencies from criminal infiltration, or protecting the physical and strategic assets of our agencies. Risks to integrity may be the result of a careless act, or even an act that was well-intentioned but ill-judged.

Managers have a role to play in ensuring that agencies have strong reputations for doing the right thing, in the right way. This requires managers to think broadly about what risks their agencies face.

Common integrity risks

Reducing the incidence of criminal breaches of integrity is important. Managers need to be aware of, and put in place, mitigation strategies to deal with risks of this kind.

But we should also be thinking more broadly. An employee may be upset by a recent staffing decision and therefore become unproductive or think about leaking damaging information. This may be a risk to integrity, too.

Motivating factors

There is no single, exhaustive list of the factors that may motivate an employee to commit improper conduct. Research shows, however, that factors can include:

Revenge

- following a negative incident such as a workplace dispute, demotion or termination of employment

Financial reasons

- seeking financial gain
- experiencing high levels of personal debt
- pursuing own business interests

Disgruntlement

- affected by organisational change
- dissatisfaction with organisational policies
- resentment due to unmet career expectations
- lack of promotion opportunities
- change leading to diminished or unfair responsibilities
- imposition of sanctions for previous misconduct
- being offered or not offered a redundancy package

Coercion

- manipulation by others, including blackmail
- social and familial pressures
- misplaced loyalties

Relationships

- poor relationship with manager
- poor relationships with co-workers
- family relationship breakdown
- criminal associations
- political ideology

Psychosocial factors

- drug and alcohol abuse or dependency
- addictive or compulsive behaviours such as gambling
- risk-taking behaviour

While factors of this kind may explain, or even help to predict, behaviour that challenges integrity within an agency, they do not excuse such behaviour.

Red flags

An employee's personal circumstances, lifestyle and individual vulnerabilities are often relevant when identifying potential areas of risk related to deliberate misconduct. Some workplace behaviour is of particular interest and may be predictive of future behaviour if observed on a regular basis or without reasonable explanation.

Warning signs that might indicate an individual has become an integrity risk include:

- signs of a financial windfall—living beyond demonstrated means, such as buying expensive items
- indications that they are associating with criminal entities or taking illicit drugs
- changed attendance patterns—a sudden change of working hours or attendance at work, absenteeism, or tardiness
- a reduction in performance—difficulty meeting deadlines, distraction, poor decision-making, difficulty remaining focussed on work-related tasks
- inappropriate social behaviour—conflict with co-workers, bullying, lack of empathy, argumentativeness, abrasiveness, domineering or offensive behaviour
- difficulty conforming to workplace rules and expectations
- displays of addictive behaviour such as drug and alcohol misuse, or problem gambling
- responding inappropriately to constructive criticism
- displaying an undue sense of entitlement, seeking preferential treatment
- working during leave or outside hours when not clearly needed
- complaints being lodged about them, including bullying and harassment
- misuse of agency resources—such as misusing cabcharges or credit cards, accessing databases not related to duties, extensive use of photocopiers or printers, inappropriate use of ICT systems, failure to return equipment
- engaging in reckless or impulsive behaviour
- threatening or engaging in retaliatory behaviour against others
- making humiliating, insulting or harassing remarks about others.

A red flag does not necessarily mean that an employee is actually compromising the integrity of the agency, although some of the actions listed above would be a breach of the Code of Conduct in their own right. The behaviour may only indicate that managers should be more conscious of the actions of the employee and perhaps intervene to establish whether work-related factors are driving the behaviour. Managers should be on the lookout for patterns of behaviour that indicate an employee might be becoming a substantial integrity risk.

In many cases the best approach to dealing with an issue will be to offer the employee support through a difficult period. If the behaviour is identified early, counselling, perhaps with the assistance of the Employee Assistance Program, will often be sufficient to deal with the issue.

A toxic team culture

While the behaviour of an individual employee may indicate a potential integrity risk, local workplace cultures can also develop within teams that represent a potential risk.

The characteristics of these teams often include:

- the team is geographically isolated from the larger organisation, for example they undertake field work or work unsociable hours
- the team socialises together extensively and team members are very loyal to each other
- there is tolerance of rule breaking and poor behaviour, some of which is relatively minor—practical jokes, unprofessional language, sexualised behaviour
- team leaders may be complicit and there is not sufficient oversight from senior managers.

The first indicator of a broader integrity problem may be an allegation of sexual harassment or bullying which is difficult to investigate because team members act to protect each other. However, a culture of rule breaking rather than high professional standards, and a primary loyalty to colleagues rather than the employer, can create circumstances where corruption is tolerated and overlooked.

Adapted from: https://www.apsc.gov.au/identifying-other-integrity-risks

Culture and fraud prevention

Fostering a culture of integrity

A culture based on high standards of integrity is a core component of public service. A strong ethical culture is essential to detecting, preventing and mitigating risks to integrity.

The *Public Sector Employment and Management Act 1993* (PSEMA) articulates the requirement for NTPS employees to observe the public sector principles of:

- the administration management principle
- the human resource management principle, including the merit principle and the equality of employment principle; and
- the performance and conduct principle.

The NTPS Code of Conduct includes these elements of behaviour:

- personal and professional behaviour
- relationships between employees and government
- relationships between employees and the Legislative Assembly
- public comment
- use of official information
- use of official facilities and equipment
- financial and other private interests
- disclosure of offences against the law
- political participation
- outside employment
- acceptance of gifts and benefits
- fairness and equity
- discrimination
- employees to exercise due care
- disclosure of wrongdoing.

An agency culture of integrity is shaped by a consistent tone from the top—the messages and example set by managers in our decisions and our treatment of staff—and an underlying ethos of strong governance and professional standards.

Managers play a key role in government agencies. As individuals, managers can have a strong influence on the work cultures of their teams. They play a critical role in identifying potential risks and reporting any concerns. They are close enough to employees, procedures and processes to be able to identify risks and problematic behaviour, and to model appropriate integrity behaviour. As a group, managers influence the culture of workplaces in the behaviour they adopt and reward.

The effectiveness of the NTPS fundamentally depends on public trust in its integrity as an institution and its capacity to look after the public interest rather than its own. A values-based culture is at the heart of a high-performing and trustworthy public sector. A culture in which employees are expected and encouraged to act ethically, in which ethical behaviour is modelled for them by their leaders and peers, and in which each aspect of their work is compatible with NTPS principles, is one in which the public can have confidence.

1.1 The business case

As public servants we have an extraordinary opportunity to make a real contribution to our communities. The community and the government rightly expect us to undertake our work on their behalf conscientiously and professionally.

Exercising good judgement—understanding the options available, taking the best decision and putting it into practice—can be challenging. It is especially important that managers reflect on the relevance of NTPS principles to our jobs and the issues we face, and that managers make sound decisions.

When something goes wrong we need to act in a timely and decisive manner. This is crucial to maintain the trust of the government and the community in our ability to manage ourselves. We must address poor or risky behaviour and misconduct promptly when it is identified.

Managers need to remember that employees will look to them to demonstrate the right attitude and behaviour in the workplace. Managers are responsible for:

- identifying and managing areas of potential risk
- being open to scrutiny and transparent in decision-making
- helping people in their teams to manage real or potential conflicts of interest
- reporting and addressing misconduct and other unacceptable behaviour in a fair, timely and effective way
- being able to demonstrate that resources have been used efficiently, effectively, economically and ethically.

Managers should ensure that their teams are fully aware of policies and procedures relevant to conduct and professional behaviour and that they know how to report conflicts of interest and other integrity risks.

Failure to act with integrity has impacts at both the personal and organisational level. At a personal level, there are impacts on the careers of people acting without integrity and often also impacts on colleagues and members of the public.

At an organisational level, there are the administrative costs of conducting enquiries as well as costs associated with managing reputational damage—the costs associated with a loss of confidence from the public, from other agencies and from the government. Further impacts may include damage to the viability of programs and policies, with flow on effects to industry and the private sector.

1.2 Taking steps

The identification and management of any form of risk is the most cost-effective strategy to mitigate that risk.

Prevention is better, and cheaper, than cure. The cost of identifying, investigating and sanctioning individuals who have breached their obligations can be substantially avoided by implementing measures that educate staff about their responsibilities. However, embedding integrity as a core component of an organisation's culture will only be effective if it is clearly understood.

REFLECT Ethical Decision Making Model

RE	Recognise a potential issue or problem	**Ask yourself:** • do I have a gut feeling that something isn't right? • do I feel this is a risky situation? **Recognise the situation as one that may involve tensions:** • between two or more of the NTPS principles • between the NTPS principles and personal values.
F	Find the relevant information & gather the facts	• what was the trigger and what are the circumstances? • identify the relevant legislation, policies and guidance (NTPS wide and agency-specific) • identify the rights and responsibilities of relevant stakeholders • identify any precedent decisions
L	Linger at the fork in the road.	**Pause to consult** • supervisors and managers • respected colleagues, peers or support services—remember privacy • talk it through, use intuition and analysis, listen and reflect.
E	Evaluate the options	**Identify consequences, look at the processes** • identify the risks • discard unrealistic options • apply the accountability test—would the decision stand up to public scrutiny/independent review? • be prepared to explain the reasons for your decision.
C	Come to a decision	**Act on it and make a record if necessary**
T	Take the time to reflect	**Review the situation:** • how did it turn out for all concerned? • learn from your decision • if you had to do it again, what would you do differently?

Sourced: https://www.apsc.gov.au/reflect-aps-values-and-code-conduct-decision-making-model

Checklist: Creating an ethical culture

What an agency can do

Develop and release a policy on the agency's commitment to the NTPS Principles and Code of Conduct and to promoting a strong integrity culture. The policy should:

- state that unethical conduct and behaviour which breaches the Principles and Code will not be tolerated
- set out the responsibilities of the agency head, senior executives, other managers and employees to create a culture that supports ethical conduct
- provide a clear view of, and strategies to promote, appropriate standards of behaviour for employees at all levels.

Ensure all employees have easy access to the agency's policies on ethical conduct and behaviour and regularly remind employees of their responsibilities.

Develop and implement policies on:

- declaring gifts and benefits
- using social media
- reasonable use of information and communications technology and other NTG resources
- conflicts of interest
- outside and post-separation employment.

Put in place effective risk management policies and procedures.

Develop clear channels for employees to report improper conduct, including details of the agency's nominated recipient is. As far as you are able, keep employees aware of action you have taken to deal with their reports.

Integrate expectations of appropriate behaviour and adherence to the Principles and Code into the performance management process.

Provide training in ethical decision-making for all employees, making sure they understand and apply the Principles and Code.

Nominate ethics contact officers to provide points of contact for employees to raise ethical issues and to provide a forum for discussion of ethical issues being raised across the agency.

What managers can do

- Make sure that your own actions model the Principles and the Code of Conduct, sending clear messages to staff about expected behaviour.
- Make sure that you are able to provide advice on:
  - ways for employees to report concerns, including formal and informal processes and external avenues
  - where to go for advice and/or support, for example, employee assistance or counselling services, agency contact officers
  - relevant internal and external review mechanisms
- Help employees manage real, perceived or potential conflicts of interest.
- Report and address misconduct and other unacceptable behaviour in a fair, timely and effective way.
- Use induction and probation to ensure new employees clearly understand what is expected of them and the standards of professional behaviour.
- Openly discuss ethical dilemmas in the workplace and how you would resolve them.
- Be a source of inspiration and guidance, helping other employees resolve ethical issues.
- Declare personal interests that may get in the way of ethical decision making.
- Reward ethical conduct and the promotion of zero tolerance of inappropriate behaviour.

What employees can do

- Uphold the NTPS Principles and comply with the Code of Conduct.
- Demonstrate personal integrity and professionalism.
- Consider whether you have any conflicts of interest.
- Seek guidance when you have difficulties resolving ethical issues.
- Raise concerns when you observe conduct that does not appear to conform to ethical standards.

Sourced from: https://www.apsc.gov.au/culture-integrity

Case studies: fraud in the public sector

Case A: the consequences of poor recruitment screening[5]

Mr B provided a false history as part of the recruitment process at Queensland Health. On his CV he falsely claimed to have tertiary qualifications and to have won awards. He did not declare that he had a criminal record for theft, that he was wanted for questioning over fraud offences, or that he had changed his name.

Over the next couple of years Mr B worked in various finance-related roles. In 2007 he then began performing higher duties as Principal Finance Officer, with reporting and monitoring responsibility for Queensland Health and ministerial grants cost centres. Within days of beginning at this level he established The Muse, a business registered to his neighbours, as a Queensland Health vendor, signing the set-up form himself as authorising officer. The following day he authorised the first of several fraudulent payments totalling $77 000 to The Muse.

His colleagues noted that his lifestyle appeared to exceed his income. He told them that he was a member of the Tahitian Royal family but needed a job to access his trust fund.

In 2008 he set up another of his own businesses, HIC, as a Queensland Health vendor. HIC was registered to him at his home address as the individual operator and owner. Between 2008 and 2011 he authorised fraudulent payments to HIC totalling over $4 million.

Numerous complaints about Mr B's conduct and work performance were made by other staff, over a period of years. Those complaints included that:

- the quality of his work was often poor and he often missed deadlines
- he gave other employees gifts (these included airline tickets valued at several thousand dollars and a $10 000 cash payment)
- he would often arrive late to work, attending anywhere from 10am to midday, and didn't complete timesheets or leave forms.

Despite recurring performance and conduct issues, Mr B was permanently appointed as a Principal Finance Officer in May 2009. In December 2010 he was placed on higher duties as the Governance Manager, Finance Branch.

Queensland Health had several other opportunities to identify Mr B as a risk:

- In 2010 an anonymous email complaint was received alleging that Mr B was defrauding Queensland Health and was due to leave Australia to start a new life. The ethics unit investigated and, on being told by Mr B's manager that there was nothing amiss, dismissed the complaint.
- In December 2010 a random audit of his credit card use revealed a number of troubling issues. These included numerous instances of transactions exceeding his $1000 limit, payment 'splitting', where a payment exceeding the $1000 limit was split into multiple transactions, each under the $1000 limit, and a number of suspicious payments.

[5] Taken from APS web site: https://www.apsc.gov.au/case-consequences-poor-employee-screening

- In January 2011, Queensland Health found that he had failed to return an official vehicle and used it over a weekend without authority; that he had travelled about 213 kilometres and incurred a speeding fine; and that he then falsified a log book entry to cover up his misuse.

It was not until December 2011, after making a single fraudulent transaction of $11 million, that his pattern of fraud was detected. Over nearly five years his fraudulent activities totalled over $16 million.

In March 2013, he pleaded guilty to a number of fraud-related offences and was sentenced to 14 years imprisonment.

The Queensland Crime and Misconduct Commission concluded that the factors enabling the fraud to continue for so long included:

1. low levels of compliance with existing policies and procedures by other staff
2. failures of financial management and accountability
3. failures in supervision and management
4. inadequate change management processes that failed to identify risk and failed to provide an effective follow-up review process
5. low awareness of the risk of fraud among staff at all levels
6. failure to properly investigate information provided in audits and complaints and evaluate it in a wider context.[6]

Lessons

- ✔ **Any agency can harbour a high risk employee.**
- ✔ **Proper pre-employment checks, including verification of CV details, are important.**
- ✔ **Misconduct or poor performance can be an indicator of more serious problems.**
- ✔ **Effective risk management procedures can solve small problems before they become big ones.**

[6] Queensland Crime and Misconduct Commission Media Release, September 2013

Case B: Conflict of interest[7]

Australian Government public servant Ms G forwarded an email containing sensitive material about the United Nations Draft *Declaration on the Rights of Indigenous People* to her daughter. She also sent four emails to a friend in Mutitjulu about dysfunction in outback Aboriginal communities at a time when these issues were sensitive and the Australian Government was considering its response.

Australian Public Service Regulation 2.1 forbids the unlawful disclosure of certain sensitive information by APS employees. A failure to comply with regulation 2.1 can lead to a prosecution under section 70(1) of the *Crimes Act 1914.*

Ms G was charged under that Act with seven counts of unlawful disclosure by a Commonwealth officer. In 2008, a jury in the Supreme Court of the Australian Capital Territory found her guilty on five counts. She was placed on a good behaviour bond for three years and fined a substantial amount.

Lessons

- **Conflicts of interest do not only arise from financial or property interests. Any situation that creates competing responsibilities can give rise to a conflict.**
- **Managers and employees need to be aware of the possibility of conflicts of interest, and take early and continuing steps to manage them properly.**
- **Integrity protocols need to address potential conflicts of interest, as well as fraud and corruption risks.**

Case C: Long-serving employees can represent a risk

People often assume that it is only new employees who take advantage of their positions. This is not the case. International Fraud Awareness Week statistics indicate that those with tenure of five years or less incur a median loss of $100 000 while those with tenure of six years of more incur a median loss of $200 000.

A case in West Australia highlights a typical scenario. That is, a café worker at a public hospital with tenure of more than 10 years was found guilty of stealing more than $186 000 in 2010.

While it was unclear for how long the theft had been occurring, it was estimated to have been five years. That theft would have been prevented had the agency heeded the review it commissioned in 2002, which itself was the result of suspicion of theft and recommended a range of actions to tighten money handling procedures.

While the WA Corruption and Crime Commission's media statement on this matter[9] was silent on the type of behaviour the Leading Hand exhibited, the third most common red flag of indicators of fraud is an unusually close association with vendors or customers. This type of behaviour is exhibited in 19% of cases.

[7] https://www.apsc.gov.au/case-d-conflict-interest

Case D: Procurement fraud

Procurement is a high risk operational area for fraud.

In October 2014, the Department of Infrastructure, now the Department of Infrastructure, Planning and Logistics (DIPL) established the Indigenous Employment Provisional Sum (IEPS) to increase employment opportunities in the NT and enhance the capacity of Aboriginal businesses in respect of construction projects.

The IEPS encouraged the employment of Aboriginal people by allowing eligible contractors to claim reimbursement of wages.

Timber & Steel Constructions was an eligible contractor to participate in the IEPS. Mr Timothy Schwab was the director and manager of the Darwin-based business, which was established in 2010. The company was awarded six contracts by DIPL that enabled claims to be made against the IEPS.

In late 2016, a DIPL staff member identified some discrepancies in Timber & Steel Construction's claims from 2015 that had resulted in excess payments of $33 460. Mr Schwab was notified by DIPL in December 2016 and repaid the full amount.

In February 2017, DIPL initiated an audit to verify expenditure against the claims by Timber & Steel Constructions. During this time, the Police had discovered that Mr Schwab had fabricated pay sheets that were submitted to DIPL for payment under the IEPS.

Mr Schwab's fraudulent behaviour resulted in 56 counts of deceptive conduct and a number of financial benefits received between November 2015 and June 2017. The total in question was $213 312.16, which included GST payments made by DIPL.

Mr Schwab was found to have acted deceptively and dishonestly in a number of ways over the period in question:

- creating pay sheets for employees who were not working for Timber & Steel Constructions at the time of the contract period;
- claiming overstated wages for employees from what they were actually being paid by Timber & Steel Constructions;
- claiming additional hours worked by employees of the IEPS;
- submitting claims for employees working on projects that were not related to the contracts of the IEPS;
- forging pay sheets for subcontractors who were claimed as employees of Timber & Steel Constructions instead of as ABN holders.

Risks and impact

- disruption to the general operations of DIPL
- increased resources and expenses incurred by DIPL to investigate the fraudulent claims
- suspension of the scheme which impacted employment in the construction sector for Aboriginal Territorians
- reputational risk and loss of confidence in the department, and more broadly the NT
- potential distrust between the agency and contractors
- obstructing the prosperity of the Territory.

Case E: Procurement fraud

Top End Health Service technical services officer John Zvimba worked in the Engineering Department at Royal Darwin Hospital (RDH) from 2 March 2015 to 24 April 2017.

The Engineering Department is responsible for overseeing all electrical, mechanical, civil and hydraulic repairs and maintenance works that are carried out at the hospital.

Mr Zvimba's role at the hospital included general supervision of the electrical trades, raising work orders in the building management system and inspecting and reviewing contractor invoices and supporting documentation submitted to the Northern Territory Government's account payable Electronic Invoice Management System (EIMS).

Mr Zvimba formed business partnerships with his co-offender, Walter Wilton, being SES Electrical NT and Shona Electrical Services.

Mr Zvimba created two new contractors – vendors – in the Department's building management system and gave codes to SES Electrical NT and Shona Electrical Services.

Mr Zvimba raised 36 work orders in the building management system in a period of six months for fictitious electrical works at Royal Darwin Hospital. He assigned the work in the government system to Mr Wilton as his business partner.

Mr Wilton created corresponding invoices and he completed and signed supporting documentation for each work order.

On receipt of invoices and attached documentation, NT Government accounts payable personnel uploaded the invoices and supporting documentation into EIMS and electronically assigned the transactions to Mr Zvimba as the verifier and coder. Mr Zvimba checked and coded each invoice in EIMS and assigned a departmental cost code.

Mr Zvimba then assigned the EIMS transactions to the Engineering Services manager for final payment approval. The manager, acting in good faith that Mr Zvimba had conducted due diligence in checking the invoices, approved payment of the invoices.

In early April 2017, the engineering services manager discovered the deceptive activities and referred the matter to police. A full forensic audit of all the works alleged to have been carried out by Shona Electrical Services and SES Electrical – the two companies that Mr Wilton and Mr Zvimba had created together – was undertaken.

The audit revealed that at no time had Mr Wilton or any other nominated tradesperson employed by those companies signed in at the Engineering Department to conduct any work at the RDH.

Parts and equipment that had been noted as replaced were not replaced and were still in original condition, showing signs of wear and tear, or the work had been performed by another contractor. None of the works invoiced by SES Electrical NT or Shona Electrical Services had been carried out.

Mr Wilton and Mr Zvimba were found guilty of obtaining a benefit by deception between October 2016 and March 2017:

- Generating and submitting 36 false invoices, work orders and other supporting documents that were all fraudulent.
- Unlawfully obtaining a total of $148 031.63 from the NT Government.

Mr Zvimba pleaded guilty to his role in the scam and was sentenced to more than four years' jail. Mr Wilton was sentenced in February 2019 to more than three years' jail.

In her sentencing remarks, Her Honour Justice Kelly said: "The Crown accepts that Mr Zvimba's moral culpability was worse than yours (Mr Wilton's), and I agree, but only for this reason: that he was an employee and that theft by a servant is considered more serious because it involves a breach of trust."

Risks and impact

- Substantial monetary loss from Top End Health Service as well as breaches of employee trust, and unlawful benefits gained from rorting system and process vulnerabilities.
- Potential staff and time resourcing required to audit and review historical data and information to determine whether other fraudulent activity had occurred, as well as implementing changes to the system and its processes.
- Reputational risk and loss of confidence in the agency and the broader NT Government.
- Clear conflict of interest in two instances:
  1) Mr Zvimba did not declare his business relationship with Mr Wilton at any time during his employment with the agency
  2) Mr Zvimba used his official duty and NT Government resources, time and information to pursue personal interests with Mr Wilton which caused detriment to a public body.
- Mr Zvimba's actions demonstrate:
  1) improper conduct, specifically corrupt conduct as defined by the Independent Commissioner Against Corruption Act; and
  2) breaches of a range of sections in the Office of the Commissioner for Public Employment's (OCPE) Code of Conduct which stipulates the basic level of conduct expected of public sector officers. This includes but is not limited to misuse of information, acceptance of gifts and benefits, and declaring financial and other private interests.
  3) Fraud by obtaining benefit by deception under Division 2 of the Criminal Code Act.
- Potential mistrust between the agency and its contractors.

References

Association of Certified Fraud Examiners (2016), *ACFE Fraud Prevention Check-Up*, Austin, USA.

Australian Public Service Commission (2018) *Case A: Consequences of poor employee screening*, Canberra ACT.

Australian Public Service Commission (2017) *Government Fraud Control Framework*, Canberra ACT.

Australian Public Service Commission (2018) *Reflect: APS Values and Code of Conduct: Decision-making model*, Canberra ACT.

Australian Public Service Commission (2018) *Checklist—creating an ethical culture*, Canberra ACT.

Australian Public Service Commission (2018) *Identifying other integrity risks*, Canberra ACT.

Australian Public Service Commission (2018) *Managing Risks—Former Employees*, Canberra ACT.

Australian Public Service Commission (2018) *Managing Risks in the Workplace*, Canberra ACT.

Colwill, C. (2009) 'Human factors in information security: The insider threat—Who can you trust these days?' in *Information Security Technical Report*, November 2009.

Cressey, DR (1973) 'Other People's Money: A Study in Social Psychology of Embezzlement', in *Criminology, Law Enforcement and Social Problems* (Issue 202), Montclair; Paterson Smith.

Deloitte (2008) *Public sector fraud: identifying the risk areas*, Dublin, Ireland.

International Fraud Awareness Week (2020), *Behavioural Red Flags of Fraud*, Austin, USA.

International Fraud Awareness Week (2020), *Five Fraud Tips Every Leader Should Act On*, Austin, USA.

International Fraud Awareness Week (2020), *Fraud Prevention Checklist*, Austin, USA.

International Fraud Awareness Week (2020), *Profile of a Fraudster*, Austin, USA.

International Fraud Awareness Week (2020), *Response to Fraud*, Austin, USA.

Northern Territory Department of Treasury and Finance, *Treasurer's Direction—Fraud Control*, Darwin, Australia.

Northern Territory Independent Commissioner Against Corruption (2019) *Frameworks and Practices for Minimising Risks of Retaliation*, Darwin, Australia.

Northern Territory Public Service Commissioner (2019-20) *State of the Service Report*, Darwin, Australia.

Freecall
1800 250 918

GPO Box 3750
Darwin NT 0801

icac.nt.gov.au

Office of the
Independent
Commissioner
Against
Corruption NT