Commonwealth Fraud Prevention Centre

Australian Government

Fraud Risk Assessment

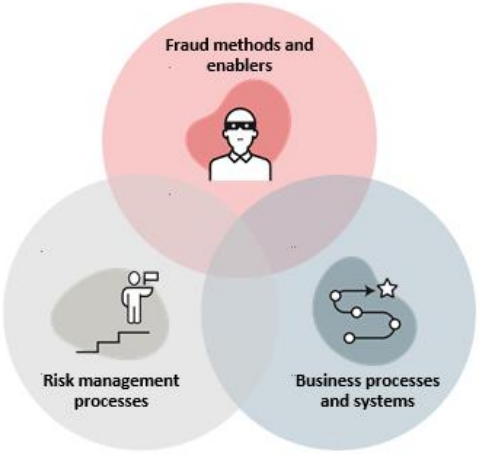
Leading Practice Guide

Table of contents

1. Introduction

Fraud is a serious, underestimated and often unchecked problem. Fraud against Commonwealth entities is driven by many factors, including vulnerabilities in policies, processes and systems that enable opportunistic individuals to take advantage. Fraud is a profession for capable and committed criminals who actively look to exploit government systems and programs. Every Commonwealth entity is exposed to fraud of some form, but because it is usually hidden from sight, constantly changing and not well understood by most people, the risks and impacts of fraud are often underestimated and overlooked. If left unchecked, fraud can seriously harm Commonwealth programs, officials, service providers and members of the public.

Fraud risk assessments shed light in dark places, assisting officials to understand the risks and enable them to make better decisions about how to manage them. If an entity knows where it is vulnerable, it is better placed to design suitable countermeasures (also commonly called controls) to prevent fraud occurring or reducing the impact when it does.



Fraud risk assessment is a specialist area of risk management. Accurately assessing fraud risk is therefore a professional exercise that requires knowledge of fraud methods and enablers, risk management processes and an entity's business processes and systems. The process requires coordination and collaboration across multiple business areas.

1.1. Purpose of this guide

The purpose of this guide is to provide Fraud Control Officers with principles and methods which have been taken from leading fraud risk assessment practices across sectors. Officers can then apply or adapt these methods to suit their individual circumstances. The guide will also help fraud specialists, government officials (including policy designers) and senior leaders better understand the fraud risk assessment process and how these assessments can benefit their entity.

Specifically, the guide will assist entities to:

- underpin their counter fraud approach with an understanding of how their organisation could be defrauded
- complete strategic-level profiling to identify areas of the organisation that are at higher risk of fraud, helping prioritise areas for further assessment
- understand the purpose and objectives of a fraud risk assessment
- understand and apply the series of interrelated steps involved in a fraud risk assessment
- co-design solutions with stakeholders to effectively treat fraud risks
- continue to build knowledge and improve capability, leading to compounding value for entities.

1.2. Definition of fraud

The Commonwealth Fraud Control Policy defines fraud as 'dishonestly obtaining a benefit, or causing a loss, by deception or other means'. Fraud against the Commonwealth may include (but is not limited to):

- theft
- accounting fraud (e.g. false invoices, misappropriation)
- misuse of Commonwealth 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 Commonwealth, or failing to provide information when there is an obligation to do so
- misuse of Commonwealth assets, equipment or facilities
- cartel conduct
- making, or using, false, forged or falsified documents
- wrongfully using Commonwealth information or intellectual property.

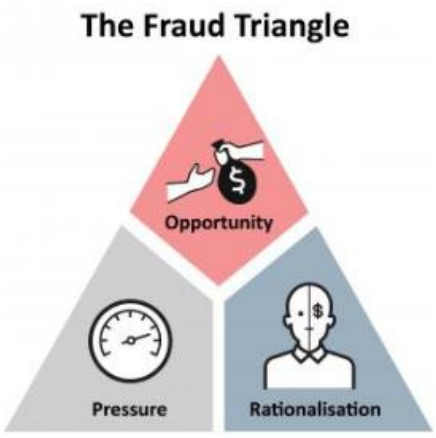
Tip: Fraud requires **intent**. It requires more than carelessness, accident or error. When intent cannot be shown, an incident may be non-compliance rather than fraud.

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. It may also include lost access rights, opportunities for employment or harm to others. Similarly, a **loss** is not limited to only meaning a financial or tangible loss. It may also include lost access rights, opportunities for employment or harm to others.

Fraud can also include some forms of **corruption**, particularly where a party obtains a benefit or the Commonwealth incurs a loss; for example, collusion between a Commonwealth official and a contractor.

1.3. The fraud triangle

The 'fraud triangle' is a model which is commonly used to explain why an individual might commit fraud. It describes three key components that contribute an individual's decision to do something fraudulent: opportunity, pressure and rationalisation.



Opportunity

This refers to a situation where an individual sees the opportunity to commit a fraud by circumventing or exploiting weaknesses in existing fraud countermeasures.

Pressure

This can be described as the things that drive a person to commit fraud. Common examples include financial pressures, gambling addictions, substance abuse or simply a person's greed or desire for financial gain. The growth in social media use has contributed to an increase in the prevalence of social anxiety and 'status envy'. These problems can incentivise individuals to commit fraud in order to demonstrate a lifestyle of wealth and status.

It is important to note that pressure varies over time and otherwise trusted employees and suppliers can turn to fraud if their circumstances change.

Rationalisation

This refers to an individual's justification for committing fraud. In simple terms, they find a way to make it okay to perform the fraudulent act. Such rationalisations include:

- "I'll pay it back later"
- "No one will even notice it's gone"
- "I deserve it"
- "I pay enough tax"
- "I'm doing it for my family"

1.4. Thinking like a fraudster

It helps to think like a fraudster when conducting fraud risk assessments, when evaluating processes and examining the effectiveness of countermeasures. Adopting an overly optimistic mindset can lead to an underestimation of fraud and its potential impact on government systems and programs.

The fraud risk assessment process should consider the common methods employed by fraudsters, and look for vulnerabilities in programs or functions that motivate and enable fraudsters. This will involve challenging assumptions to identify creative ways to circumvent countermeasures just like fraudsters do. **Annex A** provides eight Fraudster Personas which can help entities when examining processes, systems and countermeasures from the perspective of a fraudster. Understanding these personas will help entities consider the methods a fraudster might use to target a function or program, or get around a countermeasure.

Tip: Fraudsters often exhibit behaviours from several different personas. For example, they may deceive a public official, impersonate another individual, fabricate evidence and then conceal their activity.

Visit CounterFraud.gov.au for more information on these Fraudster Personas including case studies.

1.5. Summary of the fraud risk assessment process

For the purposes of this guide 'fraud risk assessment' is defined as a standard business process which enables entities to identify, analyse, evaluate and treat fraud risks which may be inherent to their business functions. The process is not one activity, but a series of interrelated steps that periodically recur:

Risk identification

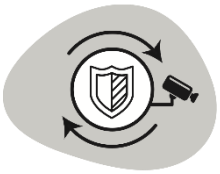
There are different approaches to identifying fraud risk which are provided in this guide. However, they all fundamentally aim to articulate how fraud actors might apply known fraud methods against business processes. Once identified, fraud risks should be articulated in a concise and consistent manner.

Risk analysis

This step involves documenting and analysing the different countermeasures currently in place to mitigate the identified risks. The effectiveness of existing countermeasures must be scrutinised in close collaboration with the business as not all will necessarily have a material effect on the risk. This step also involves estimating the level of the fraud risks based on their likelihood of occurring and their consequences if realised.

Risk evaluation

This involves fraud risk owners (see Section 2.4) evaluating whether fraud risks are within stated tolerance levels and what further action, if any, is required. This might involve doing nothing more than maintaining existing controls and monitoring the risk, through to developing new countermeasures and changing business processes.



Risk treatment

For those fraud risks which are outside stated tolerance levels, fraud risk owners must consider the most appropriate risk treatment options by balancing the potential benefits of new or enhanced countermeasures against the costs and effort of implementation and administration of those countermeasures.

1.6. Legislative requirements for fraud risk assessment

Fraud risk assessments provide assurance that public funds are being managed in an accountable manner and that the potential harms of fraud are being actively mitigated. Importantly, the *Public Governance, Performance and Accountability Act 2013* (PGPA Act) requires entities to establish appropriate systems of risk management and internal control. Consistent with the Commonwealth Fraud Control Framework and the Commonwealth Risk Management Policy[1], fraud risk assessments should be an integral element of an entity's governance and policy arrangements. These arrangements should prescribe how risks are reported and how risk management processes are embedded into key business processes.

[1] The Commonwealth Risk Management Policy requires an entity to develop a risk management framework that provides the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the entity.

The Commonwealth Fraud Control Framework requires each entity to determine the fraud risk assessment approach that is most appropriate for its circumstances. An entity may consider the following factors to determine the most appropriate approach:

- The criticality of the entity's programs and their relative exposure to fraud
- The size and complexity of the entity and its diversity of functions
- The geographical distribution of the entity's workforce and functions
- The rate of technological change
- Time and resourcing constraints.

1.7. Capability maturity in fraud risk assessments

Commonwealth entities can have varying levels of capability maturity with regards to fraud prevention and conducting fraud risk assessments. This can be driven by factors such as entities' relative levels of inherent fraud risk and executive commitment to fraud prevention activities. Entities should try to progressively mature their fraud risk assessment capabilities as a key component of their fraud control plans.

Tip: Entities with programs that may carry inherently high fraud risks are encouraged to develop fraud risk assessment processes that are specific to these programs. It is particularly important for the fraud risk assessment process to be incorporated across a program's lifecycle: from planning and design to implementation and delivery.

Refer to the Commonwealth Fraud Prevention Centre's guide on building a counter fraud investment case for practical advice on seeking new investment and resources.

2. Core foundations for leading practice

The following five conditions support and underpin leading practice in fraud risk assessment:

- strong leadership
- effective fraud control planning
- supported and capable Fraud Control Officers
- accountable fraud risk owners
- strategic direction and oversight.

2.1. Leading practice requires strong leadership

It is essential for senior officials to demonstrate a genuine commitment to controlling the risks of fraud in their entity's functions and programs. This level of commitment will make sure sufficient resources and effort are applied to the fraud risk assessment process. Strong leadership requires decisions to be made, to allocate tasks to specific people and to provide them with the authority to carry out these tasks. It also makes sure all staff take full responsibility for their role in the prevention of fraud in their entity.

Section 10 of the *Public Governance, Performance and Accountability Rule 2014* (PGPA Rule) requires Accountable Authorities to provide a certification in their annual report that a fraud risk assessment has been conducted and a fraud control plan has been prepared for the entity. An entity should also assign overall responsibility for fraud control to a 'Senior Fraud Officer', either as part of their normal duties or as a position with designated responsibility for overseeing an entity's broader counter fraud strategy. This will be determined by the size of the entity and the extent of fraud risks inherent in the entity's functions. For example, the Senior Fraud Officer might be an entity's Chief Operating Officer, Chief Risk Officer or a member of the entity's Risk Committee.

The main responsibilities of the Senior Fraud Officer are to:

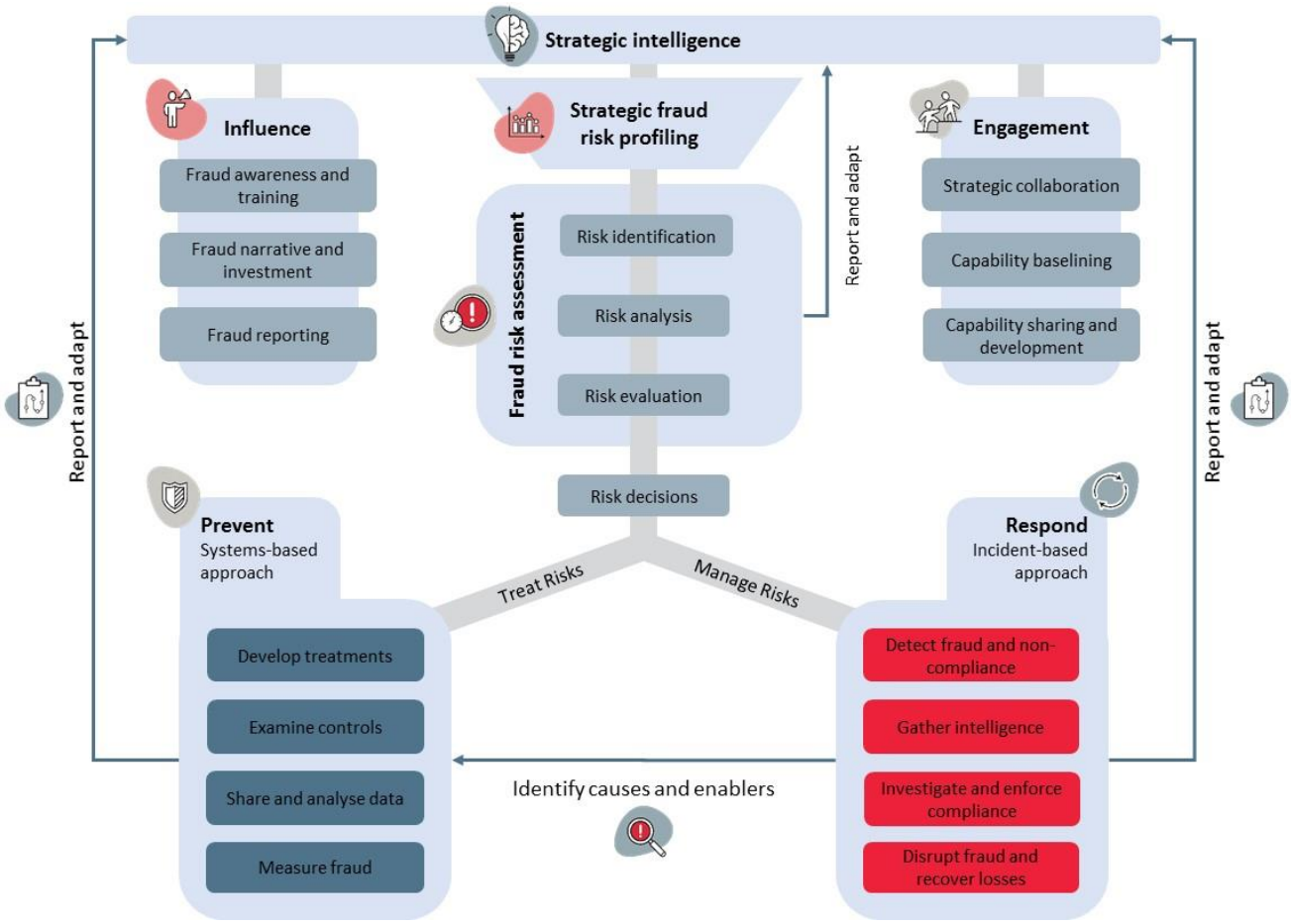
- help improve corporate understanding and commitment to the fraud risk assessment process
- confirm that fraud risk assessments are conducted to an acceptable standard, are performed in a timely manner and are sufficiently resourced
- encourage business units to actively engage with fraud risk assessments
- exercise their authority to implement change and monitor outcomes
- endorse an entity's fraud risk assessment(s) and fraud control plan(s)
- make sure outcomes of fraud risk assessments are clearly communicated across the entity.

2.2. Leading practice requires effective fraud control planning

The Commonwealth Fraud Control Framework requires the development (or update) of a fraud control plan to help entities with managing the risks identified through their fraud risk assessments. Fraud control plans can document an entity's approach to controlling fraud at a strategic, operational and tactical level, and encompass awareness raising and training, prevention, detection, reporting and investigation measures.

Figure 1 provides an example of a comprehensive counter fraud approach, illustrating how fraud risk assessments are an integral component of the approach.

Figure 1: Counter fraud approach



2.3. Leading practice requires supported and capable Fraud Control Officers

Fraud Control Officers require an entity's support to develop and implement an effective counter fraud approach. Without adequate resourcing, active support from management and top-level backing from the Senior Fraud Officer, a Fraud Control Officer will not have the capacity to conduct robust and comprehensive fraud risk assessments, potentially leaving the entity exposed to unacceptable fraud risks.

It is preferable that Fraud Control Officers, or other officials with responsibility for conducting fraud risk assessments, possess the following attributes and core competencies:

- critical thinking skills
- an ability to apply professional scepticism and to challenge assumptions
- counter fraud knowledge and experience
- risk management knowledge and risk assessment skills
- an understanding of business process management and how technology supports business processes
- sound communication and facilitation skills.

2.4. Leading practice requires accountable fraud risk owners

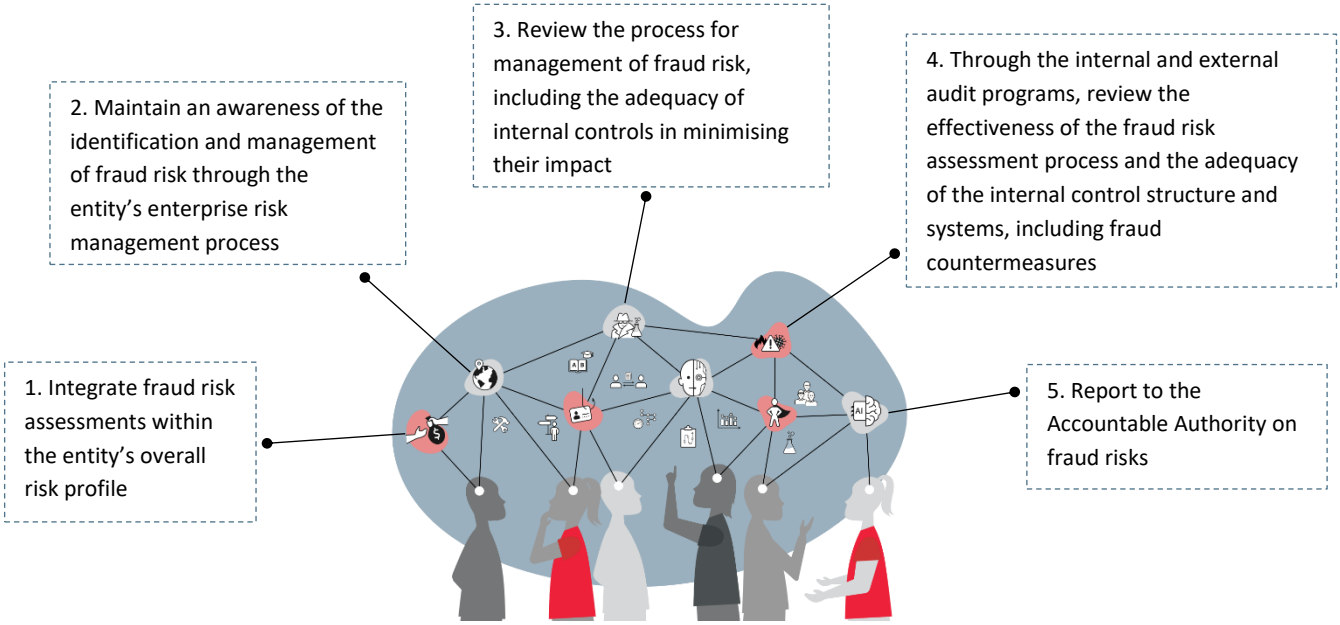
Fraud risks inherent to an entity's programs and services should be 'owned' by the relevant officials who have accountability for the functions and programs. It is the responsibility of the fraud risk owners to monitor and report on their fraud risks and make sure that countermeasures (fraud controls) are developed

and implemented in a timely manner. Sometimes these fraud controls are the responsibility of other officials in different business units, so it's important for fraud risk owners to communicate effectively with the relevant fraud control owners.

2.5. Leading practice requires strategic oversight

The PGPA Act requires Commonwealth entities to establish an audit committee and the PGPA Rule requires audit committees to review the appropriateness of an entity's systems for risk oversight and management, and internal control. Accordingly, an entity's audit committee should include fraud risk management as part of its charter and advise on key aspects (see **Figure 2**).

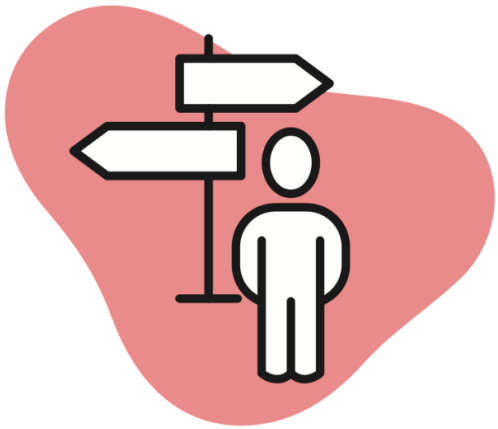
Figure 2: Role of an audit committee



Larger entities with more extensive fraud risk profiles due to the nature and size of their functions may consider establishing a dedicated fraud risk management committee. This committee should not replace senior officials' commitment to the fraud risk assessment process, but act as a forum for senior officers to better understand fraud risks and fraud countermeasures. Such a committee should include senior officers from across the entity to provide a balanced approach and help engagement with staff and relevant stakeholders.

3. Where to start

The Commonwealth Fraud Control Framework requires entities to conduct fraud risk assessments regularly and when there is a substantial change in an entity's structure, functions or activities. Substantial changes can include machinery of government changes (the merging of entities), changes to service delivery models (such as the introduction of new technologies or the transitioning into the digital delivery of services), and the design and delivery of new programs (such as eligibility payments and grant-based programs), or government responses to urgent or emergency events (such as natural disasters).



3.1. Strategic fraud risk profiling

Because some Commonwealth entities are responsible for multiple programs and business functions, conducting fraud risk assessments across these organisations can be complex, time consuming and difficult to prioritise. Strategic-level fraud risk profiling can help an entity to identify those areas of the entity that are at higher risk of fraud. This will enable Fraud Control Officers to formulate a 'heat-map' for fraud risk across the entity and to schedule fraud risk assessments on a prioritised basis.

This approach can also be adopted for national response arrangements which typically consist of multiple programs delivered by a number of Commonwealth entities. Because the size, complexity and time-critical nature of these national response arrangements make it difficult to conduct fraud risk assessments across all programs, strategic fraud risk profiling will help prioritise fraud risk assessments in programs that are at higher risk of compromise.

Strategic fraud risk profiling can use a simple scoring approach to identify those groups, divisions, branches or programs that may have inherently higher levels of fraud risk. The scoring system can be based on a number of key factors or attributes such as:

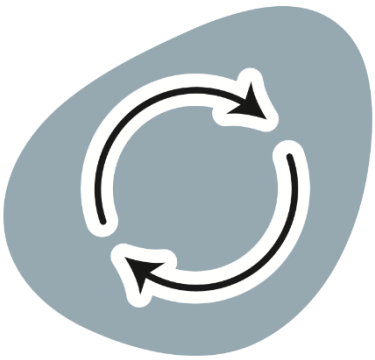
- maturity of counter fraud capability within the entity
- business unit / program budget
- operational complexity
- extent of external party involvement
- maturity of operating systems, processes and delivery platforms
- extent to which delivery is dependent upon other business units or entities
- potential to undermine government objectives and policies
- potential for reputational damage to government
- potential for harm to third parties (individuals or businesses)
- known fraud vulnerabilities
- instances of previous fraud against the business unit / program.

The Commonwealth Fraud Prevention Centre has developed a Strategic Fraud Risk Profiling Tool. To obtain a copy please contact the Centre at info@counterfraud.gov.au.

3.2. Rolling fraud risk assessment programs

Large Commonwealth entities (such as portfolio departments and large service delivery agencies) typically manage complex delivery programs and high value procurements that may carry numerous inherent fraud risks. For these entities, a rolling fraud risk assessment program (informed by strategic fraud risk profiling) may be more appropriate than a 'point-in-time' fraud risk assessment.

This will enable entities to target those high-risk functions and programs on a priority basis, and address significant changes to structure and function as they arise. This approach also allows for continual monitoring, reporting, reassessment and improvement of fraud risk assessments and responses. For highly complex, resource-intensive or sensitive programs this is more favourable than an annual 'set-and-forget' approach.



3.3. Enterprise risk management

It is important that fraud risk assessments are considered in the broader context of an entity's enterprise-wide risks. For example, there is often considerable overlap between fraud, physical security and cyber security risks. This overlapping of enterprise risks means that controls and countermeasures may often intersect. For example:

- cyber security controls which manage risks to the integrity of an entity's payment processing system can be effective fraud countermeasures
- physical security controls can assist with managing fraud risks associated with the theft of portable and attractive items.

When conducting fraud risk assessments it's important to consult closely with stakeholders responsible for managing these other categories of risks, such as the Agency Security Advisor and the Chief Information Security Officer. This will avoid duplication of effort and enable the complementary use of controls and countermeasures in combating fraud, physical security and cyber security risks.

Fraud Control Officers should make themselves familiar with the following Commonwealth Government security policies which complement the Commonwealth Fraud Control Framework:

- Protective Security Policy Framework
- Australian Government Information Security Manual.

4. The fraud risk assessment process

When conducting fraud risk assessments, the Commonwealth Fraud Control Framework encourages entities to consider the relevant recognised standards, currently the *Australian/New Zealand Standard AS/NZ ISO 31000-2018 Risk Management—Principles and Guidelines* and the *Australian Standard AS 8001-2008 Fraud and Corruption Control*[2]. Entities are also encouraged to consider their own risk management framework.

This guide describes methods and processes consistent with both the relevant standards as well as international and domestic leading practice approaches.

The fraud risk assessment process is broken down into the following four key steps:

Risk identification **Risk analysis** **Risk evaluation** **Risk treatment**

4.1. Identifying fraud risks

Identifying fraud risks should be a creative process. There can be a temptation to be defensive and argue away risks, but this is a process of finding out what could go wrong – thinking like a fraudster. Identifying fraud risks should be viewed as a positive outcome.

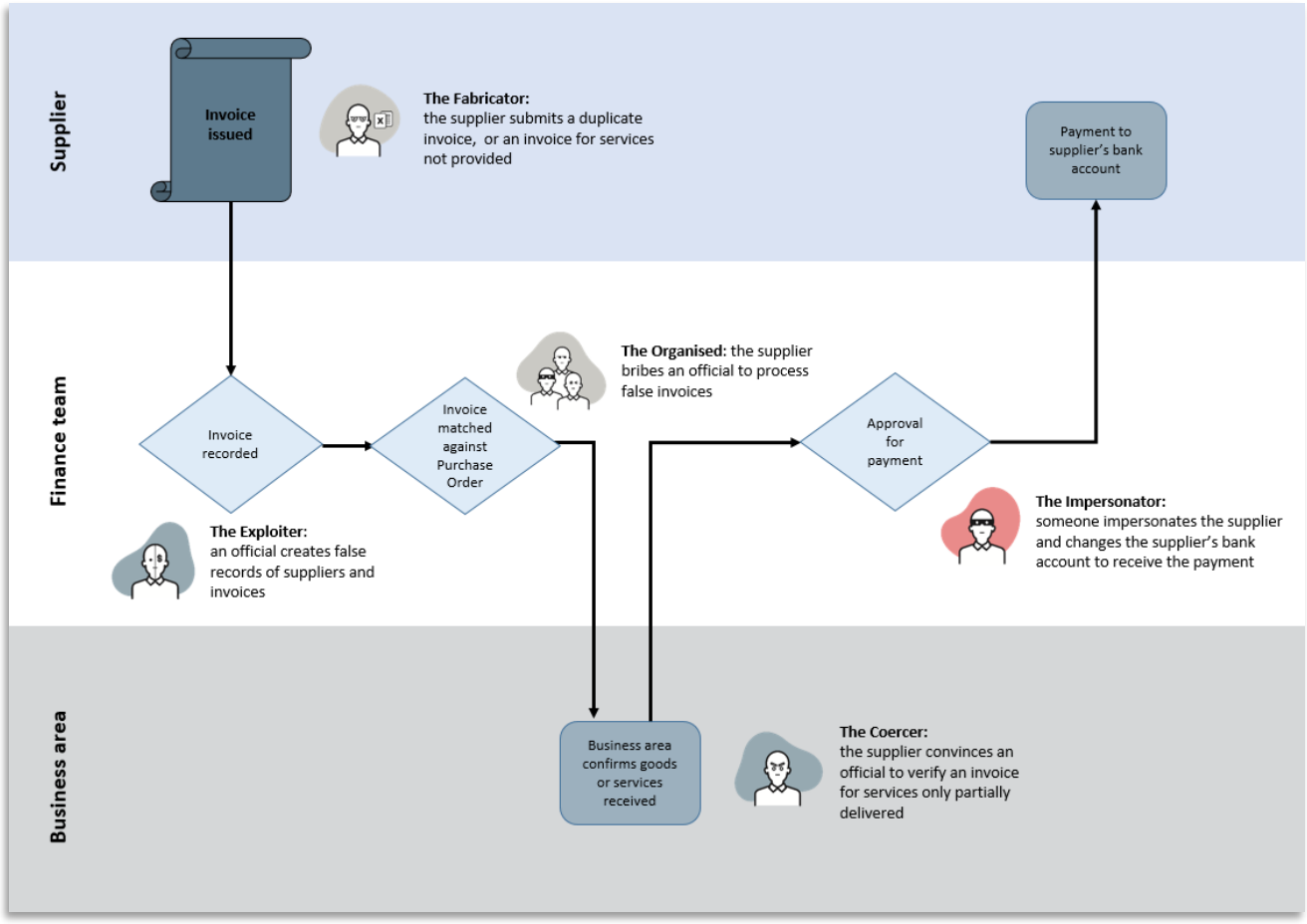
The first step in the risk assessment process, as prescribed in *AS/NZ ISO 31000-2018*, is to establish the context of the function or program being assessed through communication and consultation. This involves understanding the business processes and procedures associated with these functions such as:

- the prescribed process to receipt goods or services and pay suppliers' invoices
- the procedure followed to verify the identity of an individual or entity
- the methods to assess the eligibility of an individual or an entity to receive a payment
- the process to evaluate tenders submitted by potential suppliers of goods and services to an entity
- the standard operating procedure to approve and process pay increments to an entity's employees.

By understanding these business processes and procedures it is possible to identify the fraud risks which may be inherent in these pathways. **Figure 3** below provides an illustration of where fraud risks in an invoice payment process might be identified using Fraudster Personas. **Annex B** provides an example of a more complex hypothetical government program, and illustrates how to combine business process mapping and Fraudster Personas to identify fraud risks.

[2] **NOTE**: AS 8001-2008 is currently under review.

Figure 3 – Invoice payment process



There are a number of approaches that can be used to establish the context and identify fraud risks inherent in an entity's functions. The choice of approach will depend on a range of factors, such as size and complexity of an entity's functions, the geographical distribution of the entity's workforce and functions, and time and resourcing constraints. Regardless of the approach taken, it's important to identify and consult with representatives from the business unit(s) being assessed and any additional subject matters experts who may contribute to the identification of risks.

The following is a non-exhaustive list (in no particular order) of suggested approaches to establish the context and identify inherent fraud risks:

- Conduct interviews with senior executives responsible for corporate functions or externally facing programs which may carry inherent fraud risks. While these interviews should be structured around a set agenda, time should be allowed for exploration of topics. **Annex C** provides a guide on the matters to be covered in these interviews.
- Independently assess select processes and procedures, including a review of documentation and interviews with relevant personnel.
- Conduct a fraud risk survey using a questionnaire tailored for the entity's business units or operational functions being assessed.
- Run a facilitated workshop approach involving the input of staff from the business unit being assessed. This approach can involve structured techniques such as business process mapping, flow

charting or operational modelling. This is particularly useful when identifying fraud risks in the design phase of an externally facing government program.

- Conduct hypothetical scenario workshopping, where relevant stakeholders consider plausible methods of potential fraudsters.
- Examine fraud intelligence, previous fraud risk assessments, the results of fraud investigations, or consider case studies from other entities (this should not necessarily be restricted to Commonwealth entities).

Tip: Another approach that can help identify how someone would target a function or program, or get around a countermeasure is the 'ABCD' method:

Actors – Who are the actors involved? For example, recipients, staff, service providers.

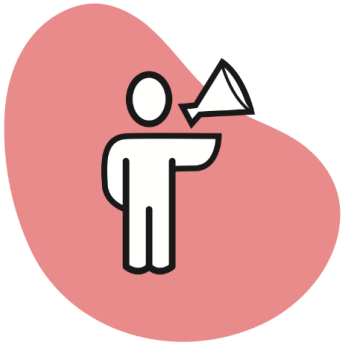
Benefits – What benefits would they gain by committing fraud?

Countermeasures – What countermeasures would they encounter?

Determined adversary – How would a determined adversary deliberately find a way around countermeasures to gain the benefit?

4.1.1. Describing fraud risks

An effective method for describing fraud risk is to consider the 'Actor, Action and Outcome'. The level of detail is important when describing fraud risks. Without sufficient detail it becomes difficult to consider the factors (i.e. actors and actions) that contribute to the fraud risk and how fraud countermeasures will specifically address these contributing factors.



A Fraud Control Officer should use their judgement in striking a balance between capturing sufficient detail and documenting a manageable number of fraud risks. This could be achieved by combining similar risks and clearly documenting the various contributing factors (actors and actions).

Annex D provides a list of key data points that can be captured when identifying and describing a fraud risk.

Tip: An example of a poorly defined fraud risk from the invoice payment process provided in Figure 1 would be:

- *"Fraud in the invoice payment process"*

The following are more accurately defined fraud risks from the same example:

- *"A service provider (Actor) submits a falsified invoice (Action) to receive a payment for services not provided (Outcome)"*
- *"A service provider (Actor) coerces an official to approve and/or process a falsified invoice (Action) to receive a payment for services not provided (Outcome)"*
- *"An official (Actor) manipulates the finance system (Action) to divert an invoice payment to their own bank account (Outcome)"*

4.2. Analysing fraud risks

An important consideration when analysing a fraud risk is the nature, extent and effectiveness of fraud countermeasures. You may be analysing a new risk for which no countermeasures have been developed or implemented, or an existing risk with countermeasures that may have known vulnerabilities. The effectiveness of any existing countermeasures can have a direct influence on the likelihood of fraud risks being realised (see Section 4.2.1).

This step in the fraud risk assessment process requires input from the business unit(s) being assessed, and any additional subject matters experts who may add value to the process. This step can be conducted in a workshop setting or structured discussion and may also incorporate the fraud risk identification step described in Section 4.1. However, for large, complex programs or functions it may be more suitable to have separate workshops or discussions for these steps in the risk assessment process.

Refer to the Commonwealth Fraud Prevention Centre's catalogue of common countermeasures for help with identifying different types of fraud countermeasures.

The following questions can assist to identify what countermeasures are currently in place or what countermeasures might be considered when treating fraud risks (see Section 4.4):

- What type of managerial oversight exists?
- How do you verify the evidence submitted by an applicant?
- Do you have any data matching in place?
- Who makes the final decision and are there automated workflows for decision making?
- What fraud detection controls are in place? Should there be more when considering rapid technological changes?
- Can someone lodge a tip-off or complaint?
- Are there any system audit logs?
- Are relevant policies and procedures in place and up-to-date, including those for the management and exercise of delegations and decision making?

Tip: The Commonwealth Fraud Prevention Centre has found that entities often overestimate the effectiveness of their countermeasures. Applying a sceptical mindset to countermeasures and adopting the mindset of a determined fraudster can help in considering whether a countermeasure might be overridden or avoided.

Annex F provides guidance on the categories of countermeasures used to treat fraud risks and how to measure their effectiveness.

If conducting a risk assessment in line with AS/NZ ISO 31000-2018, the analysis of fraud risks involves estimating the 'likelihood' and 'consequence' of the individual risks. A risk analysis matrix can then be used to match the combination of likelihood and consequence to provide an estimation of the current risk rating. **Annex E** provides an example of a risk analysis matrix.

> **Tip:** An alternative to using a risk analysis matrix to estimate the level of fraud risk is applying a scoring system against the estimation of likelihood and consequence which will provide a fraud risk score. The Commonwealth Fraud Prevention Centre has developed a Standardised Fraud Risk Tool that uses such a system. To obtain a copy please contact the Centre at info@counterfraud.gov.au.

Annex D provides a list of key data points that can be captured when analysing a fraud risk.

4.2.1. Estimating the likelihood of fraud

As highlighted above, an essential consideration when assessing a fraud risk's likelihood of being realised is the nature, extent and effectiveness of fraud countermeasures. There are a number of other factors which can be considered including:

- the volume of financial transactions associated with a business function or payment program
- the range and type of access points to the business function or payment program and the extent to which these are automated
- the nature and quantum of the potential benefit to the fraudster
- previous history of fraud against the business function or payment program (is there a known organised crime threat?)
- public awareness of an eligibility payment program
- time scales (for example, what is the duration of the function or program).

An entity's risk management framework should provide guidance on how to quantify the likelihood of a risk occurring.

4.2.2. Estimating the consequence of fraud

An entity's risk management framework should provide guidance on estimating the consequence of fraud risks, should they be realised. The measurement of the consequence of fraud is commonly based on the level of financial loss that might occur as the result of a single incident, or through cumulative losses from several incidents over a period of time. Government entities generally lose between 0.5% and 5% of their spending to fraud and related loss, based on international estimates.

Fraud incidents also involve non-financial consequences that should be considered:

- **Human impact** - fraud can be a traumatic experience that often causes real and irreversible impacts for victims, their families, carers and communities. It can also lead to a reduction in an entity's staff welfare and morale.
- **Government outcomes impact** - fraud undermines the government's ability to deliver services and achieve intended outcomes.

- **Reputational impact** - fraud can result in an erosion of trust in government and industries, and lead to a loss of international and economic reputation.
- **Industry impact** - fraud can result in distorted markets where fraudsters obtain a competitive advantage and drive out legitimate businesses.
- **Environmental impact** - fraud can lead to immediate and long-term environmental damage through pollution and damaged ecosystems and biodiversity.
- **Security impact** - fraud can undermine national defence and security.
- **Business impact** - costs for dealing with fraud go well beyond the direct financial loss and can include investigation and response costs as well as potential restitution.

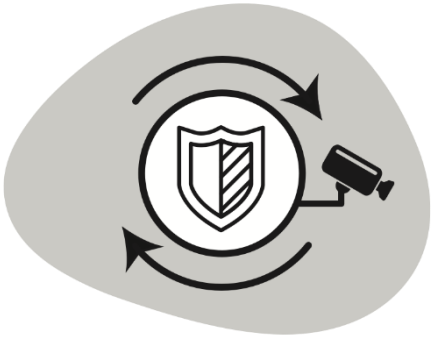
4.3. Evaluating fraud risks

Once an entity's fraud risks have been rated in the analysis step, these risks are evaluated against the entity's risk appetite and tolerance, which can be defined in an entity's risk management policy and framework[3]. The nature of an entity's business functions will determine its tolerance to fraud risks; for example, large service-delivery entities may have a greater tolerance to fraud risk owing to a higher level of risk inherent to their functions and programs. On the other hand, entities with responsibility for regulatory compliance and law enforcement will likely have a much lower tolerance with regards to fraud and corruption risks.

Annex E provides an example of a risk management action table which can be prescribed in an entity's risk management framework and can reflect an entity's risk appetite and tolerance. The table provides instructions for fraud risk owners on the actions required for different levels of fraud risk. Officials should refer to their own entity's risk management action table when evaluating fraud risks.

It is important that the evaluation of fraud risks involves input from fraud risk owners with sufficient seniority to be able to consider the cost of countering fraud against the entity's risk tolerance. An effective risk evaluation process can assist fraud risk owners in deciding a number of possible options, such as:

- avoiding or terminating the fraud risk by deciding not to start or continue with the activity that gives rise to the risk
- accepting a fraud risk that is within the entity's risk tolerance and appetite by maintaining existing controls and monitoring the risk
- accepting a fraud risk that is outside an entity's risk tolerance and appetite by informed decision, for example it has been determined that:
  - the anticipated benefits of the activity outweigh the consequences of the risk, or
  - the costs of additional treatment, or the timeframes to implement additional treatments, would have a negative impact on the outcomes of an essential activity
- undertaking further risk analysis, such as conducting an audit or 'pressure test' of the existing countermeasures (refer Section 5.2)
- treating the fraud risk to an acceptable residual (or target) level by reducing the likelihood and / or the consequences (see Section 4.4).



Annex D provides a list of key data points that can be captured when evaluating a fraud risk.

[3] The Commonwealth Risk Management Policy requires entities to define their risk appetite and risk tolerance.

4.4. Treating fraud risks

When treating a fraud risk to achieve an acceptable residual (or target) level of risk, the options available might be to enhance existing countermeasures or to introduce new and more effective countermeasures. As indicated in **Annex F**, these countermeasures can be grouped under fraud prevention, detection or response.

> **Tip:** Treating *likelihood* or *consequence*?
>
> Most fraud countermeasures are designed to reduce the *likelihood* of fraud, but some can be targeted at reducing the *consequences* of fraud. For example, reducing the maximum amount of an eligibility payment can reduce the financial *consequences* of a fraudster who is able to successfully find a way around countermeasures designed to reduce the *likelihood* of the fraud risk occurring.

The Commonwealth Fraud Prevention Centre has developed a catalogue of fraud countermeasures as a useful resource for considering additional countermeasures or enhancing existing countermeasures. The catalogue of fraud countermeasures is available at CounterFraud.gov.au and provides:

- a summary of each countermeasure
- specific examples of each countermeasure
- an explanation of the purpose of each countermeasure
- suggested ways of measuring the effectiveness of each countermeasure
- vulnerabilities to consider for each countermeasure[4]
- dependencies (links to other countermeasures that entities can consider within a broader control environment).

When considering new countermeasures, or addressing gaps and vulnerabilities in existing countermeasures, a co-design approach will achieve greater engagement and buy-in from stakeholders. As with fraud risk evaluation, it is important to get input from fraud risk owners with sufficient seniority to consider the cost of countermeasures against the risk exposure.

Annex G outlines the 'SMART' principle as an example of what to consider when co-designing countermeasures with stakeholders.

> **Tip:** Fraud risk owners can sometimes encounter problems with fraud control owners responsible for developing, implementing and maintaining fraud controls relating to their risks. This may be because a control owner is experiencing staffing or funding constraints or they lack the requisite expertise. In these circumstances the Fraud Control Officer can assist through:
>
> - fostering productive linkages between parties responsible for fraud control,
> - providing expert advice to stakeholders, or
> - seeking strategic support from the Senior Fraud Officer to formulate solutions to impediments at the operational or program level.

[4] These are not available on www.CounterFraud.gov.au but can be provided on request.

4.4.1. Information and data sharing in fraud countermeasures

Australian Government entities are encouraged to explore data sharing opportunities when designing new fraud countermeasures. Australian Government entities hold vast amounts of data and information and unlocking and sharing data and information can be a powerful tool to prevent, detect and respond to fraud.

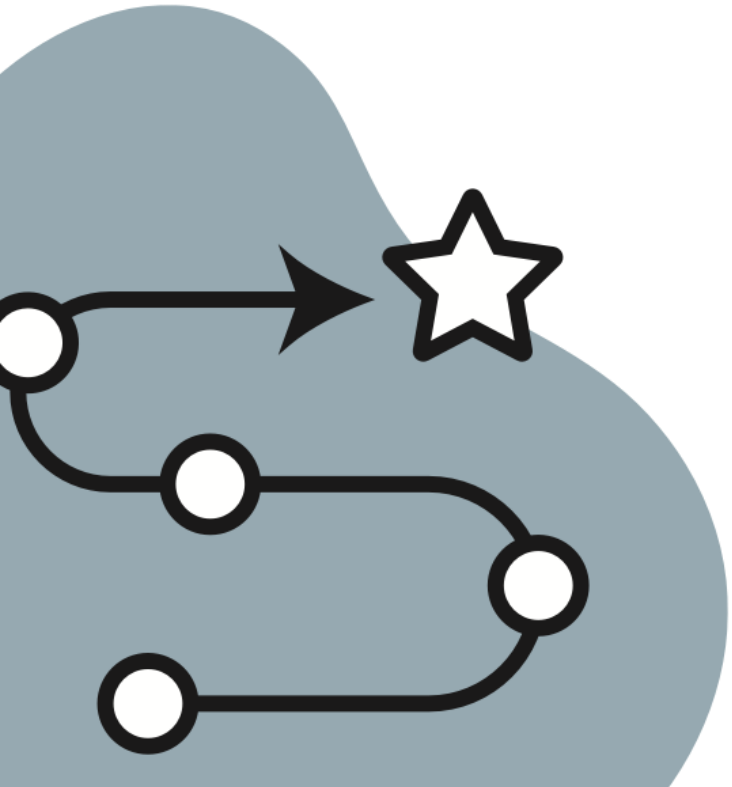
Example fraud risk 1:
"A grant applicant (Actor) *provides false accreditations* (Action) *to be eligible to receive a payment* (Outcome)."

The entity administering the grant program treats this risk by collecting data from the accreditations board to validate eligibility. Once identified, the entity also disrupts this type of fraud by sharing information under Part VIID of the *Crimes Act 1914 (Cth)* about fraudulent applicants with other grants programs.

Example fraud risk 2:
"A social welfare recipient (Actor) *provides misleading information on their income and asset status* (Action) *to be eligible to receive a welfare payment* (Outcome)."

Under a Memorandum of Understanding between the Australian Transaction Reporting and Analysis Centre (AUSTRAC) and Services Australia, specific financial transaction and financial reporting data is shared. The AUSTRAC data match will enable Services Australia to identify social welfare recipients who may not have appropriately disclosed their correct income and asset status.

Refer to the Commonwealth Fraud Prevention Centre's guide on sharing information and data to prevent fraud for practical advice and principles to consider when commencing data or information sharing activities.



5. Reporting, monitoring and review

As indicated in Section 2.1, leadership is critical to ensure activities such as strategic risk profiling and fraud risk assessments are reported, monitored and reviewed to achieve effective fraud prevention outcomes. Strategic reporting to executive committee/s can be useful leverage for influencing action to counter fraud. For example, business areas will be more inclined to take positive action if they know their decisions to counter fraud will be reported to an executive committee.

Entities should actively monitor the implementation of fraud countermeasures, because until new countermeasures are in place, those fraud risks that sit outside an entity's risk tolerance will still carry an inherently high rating. As indicated in Section 2.4, fraud risk owners will be responsible for making sure the countermeasures for their risks are implemented in a timely manner and remain effective.

It is also essential that an entity's fraud risks are carefully monitored. Sometimes only small changes to a business process or function can alter the inherent risk rating of a known fraud risk, result in the emergence of new fraud risks, or impact the effectiveness of existing countermeasures.

5.1. Fraud risk registers

A Fraud Control Officer should use a risk register which is suitable for recording, analysing, evaluating, treating and reporting fraud risks. The risk register should be used in a manner which is consistent with the entity's risk management framework. **Annex D** provides suggested data points that can be captured in a fraud risk register.

The Commonwealth Fraud Prevention Centre has developed a Standardised Fraud Risk Tool which can be used by an entity to record and manage its fraud risks. To obtain a copy please contact the Centre at **info@counterfraud.gov.au**.

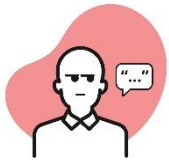
5.2. Pressure Testing Framework

The Commonwealth Pressure Testing Framework provides advice on how to examine the effectiveness of fraud countermeasures after they have been implemented through the fraud risk assessment process. Pressure testing scrutinises processes and countermeasures by considering the common methods of fraudsters, and applying an understanding of what motivates and enables individuals to commit fraud. The framework sets out key principles and materials for conducting pressure testing within Commonwealth entities. Further information about the framework is available at **CounterFraud.gov.au**.

Annex A – Fraudster Personas

The Reckless

Someone who acts recklessly (without care, responsibility or regard to the consequences of their actions) by disregarding requirements, procedures, warnings or directions.



The Deceiver

Someone who dishonestly gains a personal benefit by making others believe something that is not true.

The Impersonator

Someone who dishonestly gains a personal benefit by pretending they are another person or entity.

The Fabricator

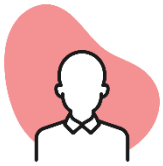
Someone who dishonestly gains a personal benefit by inventing or producing something that is false.

The Coercer

Someone who dishonestly gains a personal benefit by influencing, manipulating or bribing another person to act in a desired way.

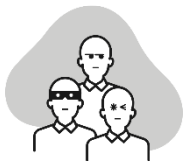
The Exploiter

Someone who dishonestly gains a personal benefit by using something for a wrongful purpose.



The Concealer

Someone who dishonestly gains a personal benefit by preventing their actions from being seen or known about.

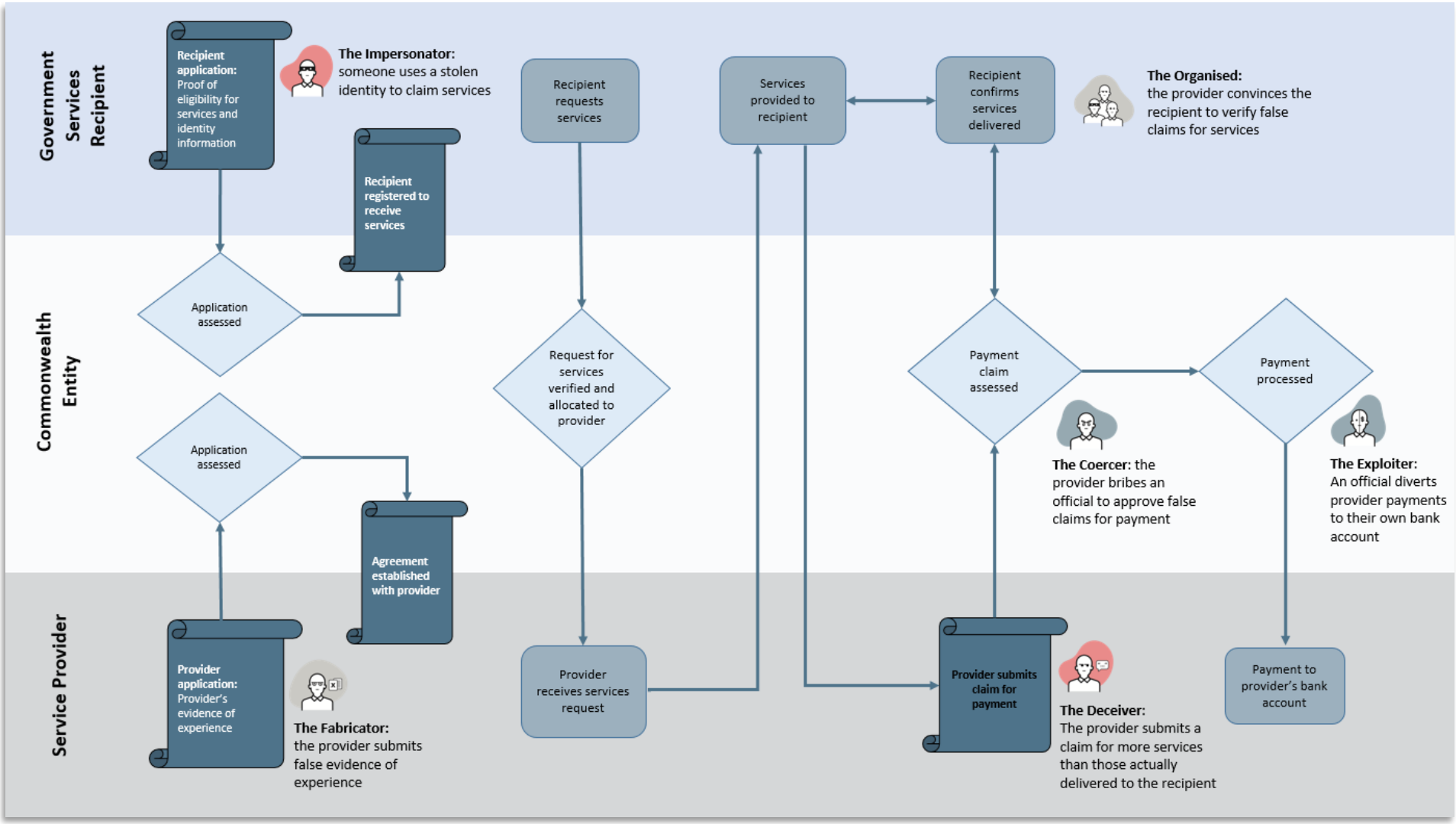


The Organised

Groups who dishonestly gain a benefit by using any combination of the other methods in a planned, coordinated and sophisticated way.

Annex B – Fraud risk points in a complex business process

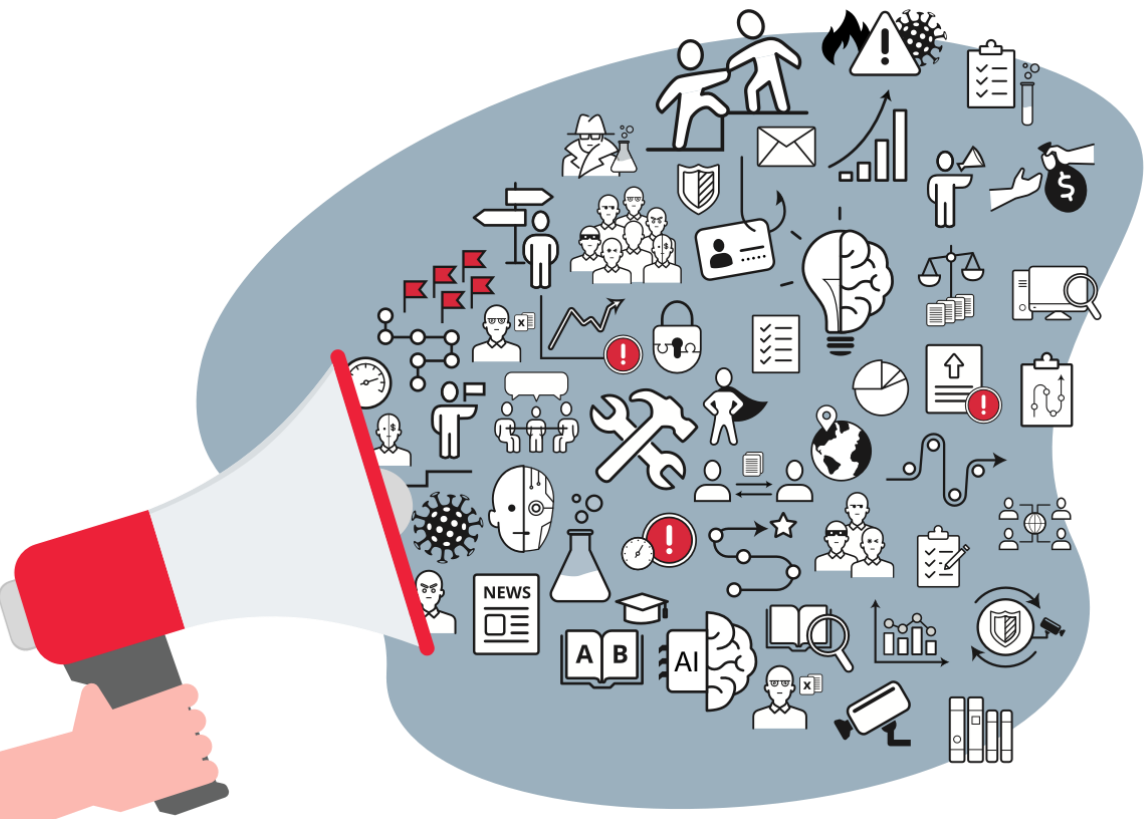
This business process map for a hypothetical government services program illustrates how to use Fraudster Personas to identify points at which someone might commit fraud against the program.



Annex C – Senior executive interview topics

When conducting interviews with senior executives the interviews should be structured around a set agenda and could consider the following questions relating to their Group/Division/Branch/Program:

- What is your opinion on opportunities for fraud in your area of responsibility?
- What are the delegations of authority and financial accountabilities in your area of responsibility?
- What monitoring and oversight mechanisms are in place?
- What are the roles and responsibilities of key personnel?
- Can you provide a high-level description of the key financial processes and systems in place?
- What are the monitoring and oversighting mechanisms?
- What is your opinion on internal pressures in your area of responsibility?
- Can you comment on the performance of individual business units?
- Are there any cultural issues or challenges (such as attitude towards mistakes), or morale issues?
- Has there been any recent changes in structure, function or systems?
- Do any of your business have high levels of staff turnover?
- Have there been any previous incidents, including suspected and actual fraud/s?
- Are you able to share the results of recent internal or external audits, or third party assurance reviews?
- Do staff in your area of responsibility have a good awareness of entity fraud control arrangements, including mechanisms for reporting suspected fraud and misconduct?
- Are there any concerns you have or any other relevant issues you wish to raise?



Annex D – Fraud risk data points

Risk identification

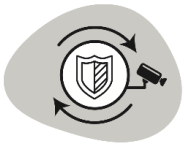
- Risk number
- Fraud risk description (actor, action, outcome / impact)
- Fraud risk owner
- Applicable Fraudster Persona

Risk analysis

- A short active title/description of each existing countermeasures (e.g. 'system controls only allow limited authorised users to change bank accounts')
- The following countermeasure attributes:
  - the owner of the countermeasure
  - the type of countermeasure (prevention, detection, response)
  - a description of what the countermeasure does to mitigate the risk
  - an effectiveness rating for the countermeasure
  - if further monitoring or assurance is required
- Control gaps or enablers (e.g. missing countermeasures, barriers to data sharing, prevalence of false identities or perverse incentives)
- An overall assessment of the control environment
- A description of the consequences of the fraud risk
- Likelihood rating (this can include the probability that the fraud risk will happen and/or the frequency the business may expect the fraud risk to occur)
- Consequence rating
- Inherent fraud risk rating (can include the rationale and/or evidence used for this rating)

Risk evaluation

- If a decision is to maintain existing controls and monitor a risk, record what this means and a future review date
- If a decision is to change or discontinue an activity to eliminate a risk, record reasons why (e.g. the costs to mitigate the risk were too high)
- If a decision is to retain a high-level risk and not apply treatments, record reasons why (e.g. the anticipated benefits of the activity outweigh the consequences of the risk, or the costs of additional treatment, or the timeframes to implement additional treatments, would have a negative impact on the outcomes of the activity)
- If a decision is to undertake further risk analysis, such as conducting an audit or 'pressure test' of the existing countermeasures, record the action to be taken and when this will be completed
- If a decision is to transfer a risk, record the new owner and when it will be transferred



Risk treatment

- If a decision is to treat a risk, record:
  - The target risk level and the commensurate risk likelihood and/or consequence
  - A short active description of the proposed treatment or countermeasure
  - The type of countermeasure (prevention, detection, response)
  - A description of what the countermeasure will do to mitigate the risk
  - A description of the implementation
  - The treatment owner
  - The implementation timeframe

The Commonwealth Fraud Prevention Centre has developed a Standardised Fraud Risk Tool which can be used by an entity to record and manage its fraud risks. To obtain a copy please contact the Centre at info@counterfraud.gov.au.

Annex E – Risk decision tools

Risk Analysis Matrix (example only)

Consequence	Likelihood				
	Rare	Unlikely	Possible	Likely	Almost Certain
Catastrophic	Medium	Medium	High	Extreme	Extreme
Major	Low	Medium	High	High	Extreme
Moderate	Low	Low	Medium	Medium	High
Minimal	Trivial	Low	Low	Medium	Medium
Insignificant	Trivial	Trivial	Low	Low	Medium

Risk Management Action Table (example only)

Risk rating	Level of action required
Extreme	The risk is beyond the entity's risk tolerance and appetite and must be immediately mitigated or avoided. Regular review and reporting of the risk needs to be provided to Senior Executive and all relevant stakeholders.
High	The risk should be mitigated or avoided, unless the anticipated benefits of the activity outweigh the consequences of the risk. Regular review and reporting of the risk needs to be provided to relevant stakeholders, and senior executive at their discretion.
Medium	The risk may be acceptable and regular review and reporting of the risk needs to be provided within the relevant business unit and to affected stakeholders.
Low	The risk is generally acceptable but must be monitored to make sure that the risk rating does not change.
Trivial	The risk is acceptable.

Annex F – Fraud countermeasures

Countermeasures are individual measures, processes or functions that help entities prevent, detect and respond to fraud. An integrated assembly of countermeasures make up a control environment. There are three high level categories of countermeasures:

Prevention

Prevention countermeasures are the most common and cost effective way to mitigate fraud. They reduce the likelihood and consequences of fraud by preventing or limiting the extent of the risk occurring.

Prevention countermeasures can include people or process countermeasures to increase transparency and influence behaviours, or processes and technology-based countermeasures to stop or limit fraudulent activity.

Detection

Detection countermeasures can help to identify when fraud has occurred. They can help disrupt additional fraud and mitigate the consequences. Detection countermeasures are not as cost effective as prevention countermeasures. However, if detected early, the impacts of fraud can be significantly reduced.

Detection countermeasures can include people and process countermeasures such as fraud aware staff and tip-off processes, or technology-based countermeasures such as fraud detection programs.

Response

Response countermeasures respond to fraud after it has occurred. They help to reduce the consequences or disrupt additional consequences. Response countermeasures are not as cost effective as prevention or detection countermeasures. However, if implemented effectively, the present and future impacts of fraud can be significantly reduced.

Response countermeasures can include people and process countermeasures such as trained fraud investigators and investigation processes, or technology-based countermeasures such as audit logging and surveillance.

Further information about specific strategies and fraud countermeasures is available at CounterFraud.gov.au.

When assessing the effectiveness of the countermeasures, it can be useful to anticipate the behaviour of a fraudster (such as provided in **Annex A**). Applying a sceptical mindset helps you consider whether a fraudster could override or find a way around a countermeasure. Trying to answer the following questions can help in assessing the effectiveness of countermeasures:

- What is the objective of the countermeasure and its unique role in managing the risk?
- What assumptions were made about the purpose and effectiveness of the countermeasure?
- Does the countermeasure work as designed? How do you know?
- Is the countermeasure relevant and up-to-date?
- Is the countermeasure automated or applied by people? If applied by people, how do you know they are applying the countermeasure consistently or correctly?
- What are the activities that support or enable the countermeasure?

- Are there backup countermeasures or fail-safes that would apply if the countermeasure did not work?
- Does the countermeasure lead to any unintended changes in behaviour?

The Commonwealth Fraud Prevention Centre has developed a Commonwealth Pressure Testing Framework to guide entities on testing of the effectiveness of fraud countermeasures after they have been implemented through the fraud risk assessment process.

The following **Countermeasure Assessment Rating Table** can also help with rating the effectiveness of countermeasures. It uses qualitative and quantitative considerations when determining a countermeasure's effectiveness. The traffic light system is a useful way to communicate where countermeasures are effective or where vulnerabilities require action.

Rating	Quantitative considerations	Qualitative considerations	Action required
Effective	• The countermeasure operates as specified 100% of the time. • The countermeasure operates as specified 90-99% of the time, however there are backup countermeasures (fail-safes) in place.	• The countermeasure is operating as specified. • The countermeasure clearly addresses the risk causes or consequences. • The countermeasure provides a reasonable level of assurance that objectives are being met.	• Continue monitoring the countermeasure.
Partially Effective	• The countermeasure operates as specified 90-99% of the time. • The countermeasure operates as specified 60-89% of the time, however there are backup countermeasures (fail-safes) in place.	• The countermeasure is occasionally operating as specified. • The countermeasure partially addresses the risk causes or consequences. • The countermeasure provides little assurance that objectives will be met.	• Review the countermeasure and consider action to improve its design and/or operational effectiveness. • Consider implementing backup countermeasures (fail-safes).
Ineffective	• The countermeasure operates as specified less than 60% of the time. • The countermeasure operates as specified 60-89% of the time, and there are **no** backup countermeasures (fail-safes) in place.	• The countermeasure does not operate as specified. • The countermeasure does not address the risk causes or consequences. • The countermeasure provides no assurance that objectives will be met.	• Take action to replace the countermeasure or improve its design and/or operational effectiveness. • Implement backup countermeasures (fail-safes).

Annex G – SMART principle for co-designing fraud countermeasures

The following table outlines the 'SMART' principle which can be applied to help co-design countermeasures with key risk stakeholders.

Specific	The countermeasure should have a clear and concise objective. They should also be well defined and clear to anyone with a basic knowledge of the work. Consider: who, what, where, when and why.
Measurable	The countermeasure and its progress should be measurable. Consider: • What does the completed countermeasure look like? • What are the benefits of the countermeasure and when they will be achieved? • The cost of the countermeasure (both financial and staffing resources).
Achievable	The countermeasure should be practical, reasonable and credible and they should also consider the available resources. Consider: • Is the countermeasure achievable with available resources? • Does the countermeasure comply with policy and legislation?
Relevant	The countermeasure should be relevant to the risk. Consider: • Does the countermeasure modify the level of risk (through impacting the causes and consequences)? • Is the countermeasure compatible with the entity's objectives and priorities?
Timed	The countermeasure should specify timeframes for completion and when benefits are expected to be achieved.

Glossary of terms

Accountable Authority - the person or group of persons with responsibility for, and control over, a Commonwealth entity's operations.

Countermeasure – individual measures, processes or functions that help entities prevent, detect and respond to fraud. An integrated assembly of countermeasures make up a control environment.

Entity – a department of state, a parliamentary department, a listed entity or a body corporate established by a law of the Commonwealth.

Fraud – dishonestly obtaining a benefit or causing a loss by deception or other means.

Fraud Control Officer – an official with responsibility for conducting an entity's fraud prevention activities, such as fraud risk assessment.

Fraud control owner – the official responsible for implementing and maintaining fraud risk controls. This official should maintain close communication with the fraud risk owner.

Fraud control plan – a plan outlining the treatment strategies and controls put in place to manage fraud risks and vulnerabilities in an entity.

Fraud control strategy – a document outlining an entity's strategic direction for countering fraud including dealing with emerging and future fraud risks.

Fraud risk owner – the official responsible for ensuring their fraud risks are monitored and treated with fraud controls in a timely and effective manner. This also requires close communication with fraud control owners.

Inherent risk – the rating of a fraud risk at a point in time when a fraud risk assessment is conducted. The rating is based on the risk's likelihood and consequence and relies on assessing the effectiveness of existing fraud countermeasures.

Official – an official as set out under section *Public Governance, Performance and Accountability Act 2013*.

Risk appetite – the amount of risk an entity is willing to accept or retain in order to achieve its objectives. Risk appetite is usually set out in a statement or series of statements that describe the entity's attitude toward risk taking.

Risk tolerance – the specific level of risk taking that is acceptable in order to achieve a specific objective or manage a category of risk. Risk tolerance represents the practical application of risk appetite and will be most effective when it is easily understood by all officials.

Residual risk – a risk rating being targeted once new or more effective fraud countermeasures have been successfully implemented. The new or enhanced countermeasures will be treating the risk's likelihood and/or consequences.

Senior Fraud Officer – a senior officer with overall responsibility for an entity's overall fraud control arrangements.

Strategic fraud risk profile – a strategic-level assessment that enables an entity to identify programs or functions that are at higher risk of fraud, and which require the prioritised application of a fraud risk assessment.

Commonwealth Fraud Prevention Centre

We aim to be your trusted adviser.

The Commonwealth Fraud Prevention Centre works with Commonwealth entities to adopt and further develop their capability to support effective fraud risk assessments.

Contact us at **info@counterfraud.gov.au** if you would like more information about conducting fraud risk assessments or would like a copy of any supporting fraud risk assessment tools.

CounterFraud.gov.au

info@counterfraud.gov.au

Copyright Disclaimer