



Manager discussion guide

Villain Academy

Guiding conversations with teams on fraud and corruption

Internal fraud and corruption

Overview

We all share an important responsibility to act with integrity, to stay alert to grooming risks and vulnerabilities and report them promptly.

This guide has been designed specifically to complement the 'Villain Academy' game. It supports managers in leading conversations with their teams and goes into more detail about important concepts and grey areas, such as ethical decision making, use of social media, potential risks and consequences.

Learning outcomes

The discussion guide aims to:

- support manager conversations with teams around the 'Villain Academy' game and fraud and corruption prevention
- encourage a deeper and balanced view on ethics, potential risks, impacts and consequences
- encourage a culture of honesty, integrity and accountability
- raise awareness of how our people can protect themselves and the ATO from fraud and corruption risks
- raise awareness on the subtleties of grooming
- encourage our people to report concerns to Speak Up, the ATO's central reporting hub for all internal fraud and corruption matters.

Instructions

Encourage your team to play the 'Villain Academy' game and read the supporting material, then arrange time to facilitate a conversation. Use this manager guide to support you – maybe at your next team meeting!

Setting the scene

Government employees and contractors are at an increased risk of being targeted for grooming, as we have privileged access to information and decision-making powers. The game demonstrates subtleties of grooming. Sometimes, it's not always obvious that corruption is at play.

The 'Villain Academy' is a fun way to get us thinking and talking about fraud and corruption, the grey areas and the ethical dilemmas they pose. Let's start with defining fraud and corruption.

What is fraud?

The Commonwealth Fraud Control Framework defines fraud as '*dishonestly obtaining a benefit or causing a loss by deception or other means*'. A benefit includes information. For an activity to be fraudulent, it must be deliberate and lead to a direct or indirect benefit to an individual or group. Fraud can be committed by parties internal or external to the ATO.

Internal fraud can include:

- falsely claiming employee benefits
- accessing and disclosing sensitive information (for example, taxpayer, charity information) without authorisation
- falsifying qualifications
- improperly reducing a debt or other liability
- releasing funds without proper authority
- using government assets for personal benefit.

What is corruption?

The *National Anti-Corruption Commission Act 2022* describes 4 types of corrupt conduct. A person engages in corrupt conduct if they:

- are a public official and they breach public trust
- are a public official and they abuse their office as a public official
- are a public official or former public official and they misuse information they have gained in their capacity as a public official
- do something that adversely affects a public official's honest or impartial exercise of powers or performance of official duties. Any person can engage in this type of corrupt conduct, even if they are not a public official themselves.

A person also engages in corrupt conduct if they try or plan to do any of these things.

Corruption can include:

- abuse of office (for example, providing sensitive information to facilitate external fraud committed by others)
- biased decision-making by ATO officials (for example, influencing procurement processes for personal benefit or benefit of a third party)
- nepotism (for example, favouring family or friends in relation to employment)
- collusion for personal gain (for example, making favourable decisions in exchange for gifts or other benefits).

Discussion questions

1. How did the game make you think about grooming on social media? Did you learn anything new?
2. How can sharing personal information on social media put you at risk?
3. How can you spot fraud or corruption attempts on social media?
4. When would you report a grooming incident on social media if it happened to you?
5. What are some examples of grooming vulnerabilities for ATO employees?
6. What are some barriers to reporting integrity concerns?
7. How could someone justify accessing taxpayer information without a business reason to do so?
8. What are the potential outcomes of being involved in fraud or corruption?
9. How can you protect yourself and your social media accounts from grooming?

Key talking points

The talking points provide more information to address the questions above.

Sharing information on social media

While social media is a valuable tool, it can also expose you to fraud and corruption risks if not used properly and responsibly. The more personal information on your social media profiles, the more you could be targeted by those seeking to do harm.

Some ATO roles and areas are more appealing to those who want to infiltrate the ATO. This includes high risk roles, and roles in payroll, security, auditing, and investigations.

The [Social media CEI](#) explains how to use social media privately and professionally and what your responsibilities are. It is fine to use social media for personal and professional purposes, as long as you follow the ATO's policies and guidelines. Be sure to review your privacy settings often, be aware of potential [risks](#) and how to manage them appropriately. Use your own judgment and common sense when deciding how much information to reveal online, such as hobbies, opinions or personal issues.

Identifying red flags

Red flags are behaviours or situations that could signal potential fraud, corruption or serious wrongdoing. They are *indicators*, not predictors.

In the game, you learned about red flags or indicators of risk, including:

- receiving, accessing, reading or sharing information without a genuine [need-to-know](#)

- undermining the ATO's ethical standards and values
- being overly secretive or defensive
- living beyond one's financial means
- ignoring the proper delegation process
- facing personal and professional difficulties
- having addictive habits, such as gambling or substance abuse
- receiving bribes in various forms such as gifts, favours, emotional support, secondary employment, holidays.

These behaviours do not automatically imply fraud. You need to look at the context and the facts. You also need to foster a safe and supportive environment for yourself and colleagues.

Discuss with your teams what you think some potential vulnerabilities are.

Reporting fraud and corruption

In the game, you may have found there were obvious – and not so obvious – times when your suspicions were raised.

It's easy when it's clear, such as being asked to [access taxpayer records](#) – a clear red flag. But others were more subtle and tricky, and that's why they're called 'flags'.

Imagine someone you met at the gym 'bumps' into you outside your work office and invites you for a coffee. You might think it's a coincidence and ignore it, even though it felt odd.

There is no right or wrong here, at this early stage you're unlikely to lodge a [security incident](#). But what about if it happened 3 times and their manner made you feel uneasy? Would you lodge an incident if you felt you were being approached because of your role as an ATO employee?

Or suppose you get a new gym bag from someone you befriended at the gym. You might not be suspicious then, but what if they offer you a brand-new iPhone? Or what if they add you on Facebook and start probing you about your work? Would that raise your alarm?

We make many friends in our lives and share personal details with them. Friendships take time to develop, so it's important to be aware of the various indicators of manipulation and deception. If someone seems too curious about your work and it makes you uneasy, it might be a red flag. Fraudsters are patient and cunning, and they don't always show their true colours. You won't get in trouble for reporting a concern, so if you're unsure, contact [Speak Up](#) for guidance.

What are some barriers to reporting integrity concerns?

Sometimes people hesitate to report an integrity concern, because:

- You think you need more evidence.
 - Leave the investigating to the experts in Fraud Prevention and Internal Investigations (FPIL), speak up with what you know, but don't investigate the matter yourself. You just need to tell FPIL what you do know.
- You don't think any action will be taken.
 - FPIL takes every report seriously and confidentially. All matters are triaged and referred to the most appropriate area. Sometimes due to privacy laws, FPIL are unable to advise the outcome, but be assured that all matters are followed up.

- You think your manager or other senior leaders accept the behaviour.
 - You can report directly to [Speak Up](#) via email or phone, or use the Anonymous Fraud Alert Form.
 - You can make a [Public Interest Disclosure](#) (PID). A PID provides legal protections for reporting serious disclosable conduct.

Ensure that your people know that they must report any suspected or witnessed fraud and corruption as soon as practicable.

You can help your team overcome these obstacles by:

- Making sure they know they must report any suspected or witnessed fraud or corruption as soon as possible. They can report to [Speak Up](#) directly by email, phone, or the [Anonymous Fraud Alert Form](#).
- Assuring them that they won't get in trouble for making a report and don't need evidence. If they are unsure, they can contact Speak Up for guidance.
- Reminding them that speaking up helps uphold the integrity and professionalism of our organisation and builds public trust and confidence in our work.
- Leading ethically through your actions and ensuring that staff understand your decisions and actions.
- Providing an environment for staff to feel safe to discuss and report integrity concerns. Often, matters can be resolved before they escalate into a complaint or allegation.
- Having regular discussions in your team meetings. There are a range of [tools and resources](#) you can use with your teams (including short team activities, perfect for team meetings).

More about grooming

In the game, an ATO employee was deliberately befriended by a fraudster who gradually built trust and rapport with them. Grooming can be very subtle, they are patient and use tactics to make it feel like a genuine friendship.

Quick facts about grooming:

- Stages of grooming are: 1) targeting, 2) relationship building, 3) coercion, and 4) corrupt conduct.
- Groomers ask for favours under the pretence of being good friends and exploit the basic human need for love and belonging.
- Grooming tactics are diverse. This can include building relationships and offering financial assistance or targeting people's 'need for recognition' (e.g., flashy cars and holidays), or manipulating, coercing and threatening.
- Gift giving and favours are used to make people feel good about the relationship, often starting small and building up so that you feel you 'owe' something to the groomer.
- 'Benefits' of corruption are not always monetary and are not always clearly linked to the corrupt behaviours.

Someone doing the wrong thing might rationalise their actions by thinking they're not hurting anyone personally (especially when they're targeting a business or the government) or the rules don't apply to them. There is nothing that makes fraud and corruption the right choice, no matter how it is rationalised. Your integrity, the integrity of the ATO, and trust and confidence of the public is most important.

Consequences of fraud and corruption

Acting fraudulently may result in a breach of the APS Code of Conduct or a criminal offence. Consequences may include:

- Personal consequences
 - impact on your personal reputation
 - loss of trust from family and friends
 - financial impacts such as not being able to afford rent and food.
- Professional consequences
 - termination of employment
 - reduction in classification
 - reduction in salary
 - re-assignment of duties
 - diminished future employment prospects.
- Criminal consequences
 - investigation by FPII and/or the National Anti-Corruption Commission
 - criminal investigation
 - prosecution
 - fines and jail time.

Your role in preventing and reporting fraud and corruption

- Report any suspected or witnessed fraud and corruption to [Speak up](#)
- Always maintain a professional relationship with clients, suppliers, and other stakeholders
- Be wary of anyone taking an unusual interest in what you do at the ATO
- Consider how much information you share on social media
- Report any unusual or persistent contact with individuals
- Stay up to date with your mandatory training
- Refresh your knowledge of [policy and frameworks](#) including the [Internal fraud and corruption CEI](#), [Access to taxation records CEI](#) and [Social media CEI](#)
- Look after yourself and colleagues, the [Employee Assistance Program](#) is available to provide wellbeing support
- Apply the [need-to-know](#) principle, exercise [good decision](#) making and keep [good records](#)
- Declare [conflicts of interest](#) and offers of [gifts and hospitality](#). If you engage or intend to engage in outside employment, notify using the [Outside employment form in People Connect](#)
- Report [security incidents](#)
- Report HR matters to [People Helpline](#).

For more information and resources

- [Speak Up](#)
- [Fraud Prevention and Internal Investigations SharePoint](#)
- [National Anti-Corruption Commission](#)
- [Public Interest Disclosures in the ATO](#)