Australian Government

Department of Foreign Affairs and Trade

FRAUD CONTROL TOOLKIT

For funding recipients

Version 1.3, February 2019

CONTENTS

ABOUT US

> **DFAT is responsible for protecting the taxpayer money it uses to achieve its objectives including by ensuring its use is in line with its intended purpose. By extension, DFAT's funding recipients must use funding in a way that aligns with their arrangement with DFAT.**

The Department of Foreign Affairs and Trade's (DFAT) purpose is to help make Australia stronger, safer and more prosperous by promoting and protecting our interests internationally and contributing to global stability and economic growth.

For more information regarding DFAT's objectives and functions, please visit www.dfat.gov.au

PURPOSE OF THIS TOOLKIT

This Fraud Control Toolkit provides DFAT's funding recipients with ways of developing and implementing fraud control strategies that meet DFAT's contractual requirements. The capacity of funding recipients to prevent, detect, investigate and respond to fraud can vary. As this varying capacity to manage fraud can have a significant impact on the Department's risk profile, this Toolkit has been developed to:

- help funding recipients manage fraud and highlight emerging fraud risks
- promote collaboration between the Department and its funding recipients when it comes to dealing with fraud
- ensure all occurrences of fraud and corruption are reported and addressed promptly in accordance with DFAT protocols
- help improve funding recipients' knowledge of how fraud might occur and what they can do about managing fraud risks.

DFAT emphasises to its staff the importance of actively working with funding recipients to ensure they are managing fraud risks. In pursuit of this shared commitment, DFAT expects funding recipients to establish measures that prevent and detect fraud and corruption. While it is not mandatory for funding recipients to use the tools included in this toolkit, funding recipients are obligated to clearly document and demonstrate their efforts in preventing, detecting and correcting fraud in accordance with the obligations in their arrangements with DFAT.

This document should be read in conjunction with DFAT's Fraud Policy Statement and the relevant definitions included at Annex 1.

> **DISCLAIMER:** This toolkit is designed as a guidance document, it not intended to direct funding recipients on how fraud should be managed within their organisations. Funding recipients are responsible for developing their own fraud management strategies that meet their obligations as outlined in their specific arrangement/s with DFAT and are tailored to their specific fraud risks.

DOES THIS TOOLKIT APPLY TO MY ORGANISATION?

This Fraud Control Toolkit applies to funding recipients who provide goods and services to DFAT including under the Australian aid program. DFAT's funding recipients include:

- commercial suppliers
- third party providers
- grant recipients
- subcontractors
- delivery chain partners
- bilateral partners
- multilateral partners
- other government agencies.

DFAT staff members and staff contracted to work in DFAT under labour hire arrangements should refer to DFAT's Fraud Control Plan available on the Intranet.

> **NOTE:** This toolkit does not apply to situations where DFAT directly funds partner governments. However, the principles outlined in this document can be used to reduce fiduciary risk and minimise fraud in all DFAT arrangements.

WHY IS FRAUD CONTROL IMPORTANT?

DFAT and its funding recipients operate in many challenging governance and security environments where fraud and corruption are significant risk factors. In recognition of this, DFAT arrangements stipulate terms that require DFAT's funding recipients to proactively protect their organisations from fraud.

Ensuring you have effective fraud control policies in place is integral to ensuring finances are protected, programs are delivered and trust and confidence is maintained in your organisation and DFAT's programs. Furthermore, funding recipients who minimise fraud will be more likely to maximise their performance under arrangements, and will therefore be more likely to be considered for future contracting opportunities.

THE IMPACT OF FRAUD

Globally, $2 trillion is stolen through corruption every year.

As a result, millions of people, primarily the elderly and young, are estimated to die every year.

The world economic forum estimates that the $2 trillion wasted every year could wipe out hunger ($116 billion), eradicate malaria ($8.5 billion over 7 years), bridge the global infrastructure gap ($1 trillion) and provide basic education to all children ($26 billion).

(International Monetary Fund, 2016 & World Economic Forum, 2017)

If you need to report suspected fraud, please click here for more information, or go to the 'Step 4 – Report Fraud' section of this Toolkit.

For more information on fraud control, please contact fraud@dfat.gov.au

HOW DFAT CAN HELP

DFAT's Fraud Control Section (FCS) oversees the management of fraud and corruption committed by external parties against DFAT including in relation to the Australian aid program. DFAT and its funding recipients strengthen their ability to combat fraud through collaboration.
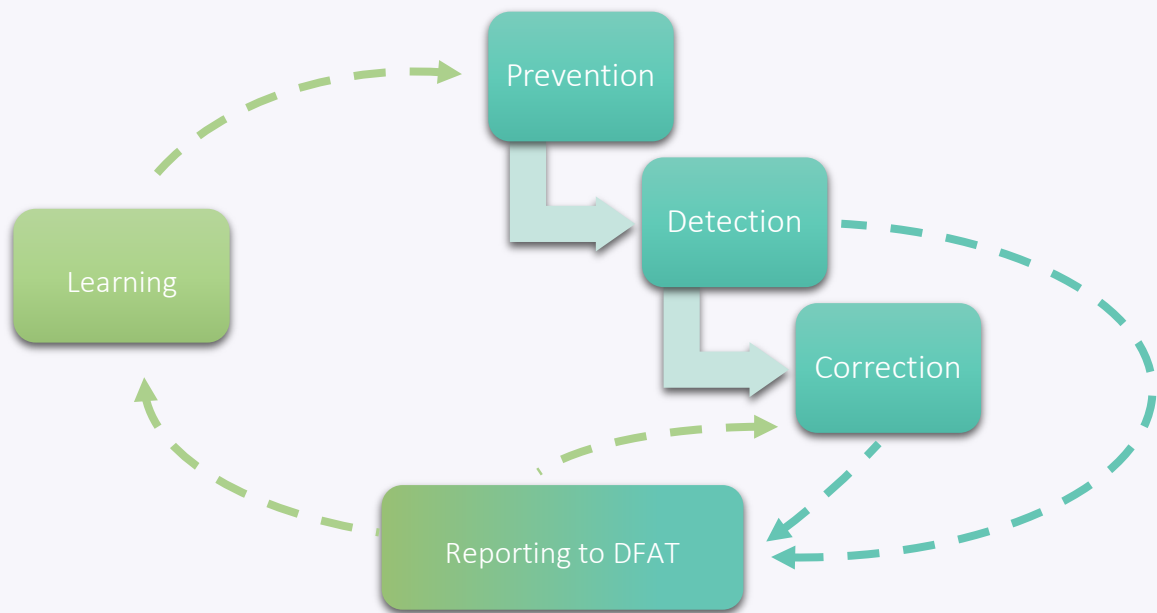
The 'Fraud Feedback Loop'

FCS will provide support to any partner facing fraud risks. A key part of this process is closing the 'Fraud Feedback Loop'. Reporting incidents of fraud to DFAT allows mutual learning from past cases of fraud and corruption to take place. It also allows DFAT to inform the investigation and correction process.

In addition to reporting fraud to DFAT, your organisation should also keep records of all instances of fraud. Using records of past incidents of fraud to inform future fraud management practice is an effective way of improving preventative measures and mitigating future risks. Maintaining accurate and readily available records is important as organisational memory will be better utilised if records can be easily accessed.

The next section of this Toolkit provides more detail on the processes funding recipients' should have in place to prevent, detect and correct fraud. At the end of this Toolkit there is a self-assessment checklist which should help your organisation identify areas that need to be strengthened to minimise the likelihood of fraud occurring and to detect it promptly if it does.

DFAT FRAUD RISK GOVERNANCE

DFAT has a range of mechanisms in place that are aimed at reducing its exposure to fraud risk. Internally, it has a Fraud Control Plan that guides its staff on how to manage fraud risks facing DFAT. There are also several committees that oversee the management of fraud. To minimise the likelihood of external fraud being committed against DFAT by its funding recipients or their sub-contractors, DFAT employs a range of measures as outlined below.

Fraud Clauses

DFAT includes a range of clauses in its arrangements to minimise risks including fraud risks. All funding recipients should ensure they are familiar with their arrangements and have policies and procedures in place to comply with DFAT's requirements (see Annex 2 for more information).

Arrangement Management

DFAT is committed to working with funding recipients to achieve mutual goals. To mitigate risks associated with outsourcing, DFAT includes requirements in its arrangements to ensure that its funding recipients have good governance frameworks in place. DFAT actively manages its arrangements in order to confirm funding recipients comply with DFAT's requirements. As part of its risk mitigation and arrangement management processes DFAT:

- ensures arrangements and guidelines are clear and unambiguous
- validates that services have been delivered
- detects and acts on non-compliance promptly
- ensures funding recipients are aware of and capable of fulfilling their fraud control responsibilities
- includes appropriate fraud control clauses in arrangements

- provides formal training to funding recipients
- publicises successful prosecutions as a deterrent to future fraud.

Policies that support DFAT's Fraud Risk Governance

While your arrangement with DFAT provides a full list of obligations, this section of the Toolkit provides an overview of policies that support DFAT's fraud risk governance. Please refer to your individual arrangement for a full list of your obligations.

Value for Money

Funding recipients are required to achieve Value for Money and spend funding in a way that is *economical, efficient, effective* and *ethical*.

If funding recipients do not apply Value for Money principles, DFAT may cancel the program or project. DFAT has developed eight Value for Money principles which all funding recipients are expected to apply. For more information on Value for Money principles, please see:

- Value for Money Principles

Preventing Terrorism-Financing

The financing of terrorism is any process by which individuals or organisations fund or make assets available to other individuals or organisations that support terrorist operations or the operatives that perform terrorist acts.

Australian laws establish serious criminal offences under the *Criminal Code Act 1995*, as well as the *Charter of the United Nations Act 1945* and its set of regulations. As per contractual arrangements, funding recipients are required to comply with Australian laws, as

well as any laws administered by the country in which they operate in, or other relevant laws. Therefore, funding recipients are expected to familiarise themselves with Australian laws, and make necessary efforts to fulfil the requirements. Funding recipients are also required to pass on similar contractual arrangements to their contractors.

Depending on the activity, and the location of that activity, some funding recipients may have additional clauses which they need to comply with. Organisations that operate in crises and war zones overseas are at greater risk of being infiltrated and exploited by terrorist groups. Funding recipients should identify the risk of terrorism-financing within their operating context, and implement controls to safeguard funds from individuals or organisations that support terrorist operations or the operatives that perform terrorist acts. This includes conducting due diligence on any contractor or grantee against the two lists maintained by the Australian Government:

1. Australian National Security Listed Terrorist Organisations, which contains a list of terrorist organisations that have been formally declared as involved in terrorism

2. Consolidated List, which contains a list of persons or entities that have been sanctioned under United Nations Security Council and Australian autonomous sanctions. Funding recipients can subscribe to receive updates of the consolidated list here.

The above-mentioned lists are not exhaustive. Funding recipients should undertake additional due diligence and vetting processes on key individuals within their organisation, as well as their contractors to ensure they have no link to

terrorist activities or organisations. By extension, the funding recipient should conduct checks on their contractor or grantee's clauses, policies, systems and processes to ensure the controls are effective enough to prevent and detect terrorism-financing.

Funding recipients should report any suspicions of the diversion of funds or assets to terrorists, or terrorist organisations, to:

- National Security Hotline – 1800 123 400
- DFAT Sanctions Section – sanctions@dfat.gov.au]
- Transnational Crime Section – transnational.crime@dfat.gov.au

Funding recipients seeking further guidance on protecting against terrorism-financing risk can access more information from the Australian Government, including the guide '*Safeguarding your organisation against terrorism-financing*', but should also seek their own legal advice. Charities and not-for-profits can access more information from the Australian Charities and Not-for-profits Commission (ACNC), including the guide on '*Protecting your charity against the risk of terrorism-financing'.*

Bribery and Facilitation Payments

When funding recipient staff accept gifts or bribes, Australia's efforts to promote good governance internationally is undermined. Furthermore, such actions could result in reputational damage for DFAT and Australia.

Included below is a brief overview of DFAT's expectations of funding recipients regarding bribery and facilitation payments. Please refer to the "Bribery and Facilitation Payment Factsheet" (Annex 5) for more information.

Bribery of Foreign Officials

It is against the *Commonwealth Criminal Code Act 1995* to bribe foreign officials. If an Australian company, citizen or resident bribes a foreign official, they can be charged under Division 70 of the *Commonwealth Criminal Code Act 1995*, and prosecuted in Australia, even if the bribery occurred overseas. All incidents of suspected bribery of foreign officials must be reported to the Transnational Crime Section:

- transnational.crime@dfat.gov.au

Banning Of Facilitation Payments

A facilitation payment is a payment of minor value provided in return for securing a minor, routine government action that should have been completed without any such payment (see S70.4 of the Commonwealth *Criminal Code Act 1995*). Facilitation payments are distinguished from bribes as they are not in any way linked to securing any decision to award, continue or create new business.

As facilitation payments can be difficult to distinguish from a bribe, DFAT funds cannot be used for facilitation payments regardless of whether it is legal in the country of payment.

If avoiding payment is likely to cause significant disruption to the delivery of a DFAT funded project or service, you should notify your DFAT contact immediately. DFAT may be able to avoid further delays by escalating the situation diplomatically.

In certain circumstances, not paying a facilitation payment can create a threat to health or safety. In such a case, the payment should be made, documented and reported to DFAT as soon as possible (see Annex 5 for more information).

Security

If your organisation is required to access, or otherwise gains access to, Commonwealth official information or security classified information, your organisation must comply with all relevant security requirements specified in the Commonwealth Protective Security Policy Framework in relation to personnel, physical and information security. Your organisation must undertake risk assessments of the environment and put in place proportional security controls to protect people, facilities and resources. For more information on the Protective Security Policy Framework, please see:

- Protective Security Policy Framework

Conducting Due Diligence on Downstream Partners

DFAT conducts due diligence on our partners and expects our funding recipients to undertake a similar process on any downstream partners they subcontract. Under standard DFAT arrangements, funding recipients are liable for the acts, defaults and omissions of the subcontractor as if they were the funding recipient's acts, defaults and omissions.

Conducting effective due diligence is an integral part of managing the risk associated with subcontracting. The downstream supplier checklist included in Annex 3 outlines steps that funding recipients should undertake on each individual and organisation they engage to ensure they are not involved in fraudulent, corrupt, coercive, collusive, obstructive practices, or other integrity violations. At a minimum, funding recipients should crosscheck organisations against the following lists:

- The Asian Development Bank's Sanction List
- World Bank Listing of Ineligible Firms and Individuals
- Australian National Security Listed Terrorist Organisations
- DFAT's Consolidated List

Funding recipients may check these lists directly or use a third party screening tool. These lists are not exhaustive so funding recipients must ensure that the checks undertaken are proportional to the risk.
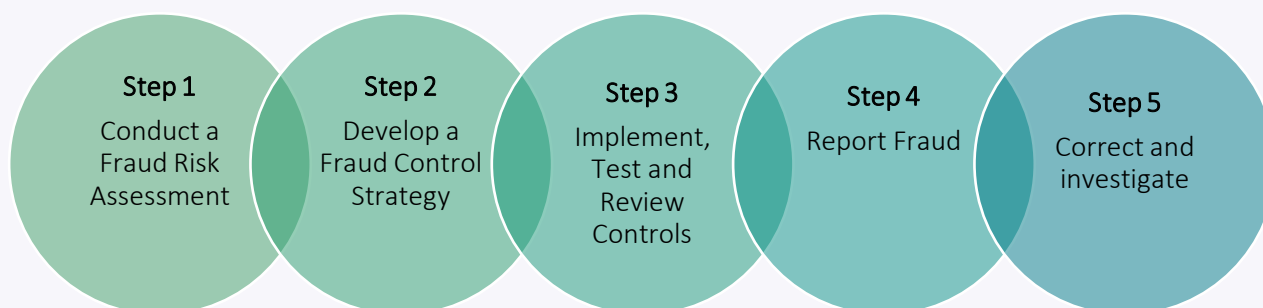
Funding recipients should be able to provide a delivery chain map of all their downstream partners if requested.

Ensure compliance by mapping contractual requirements against your internal processes and policies and then identify and address any shortcomings your organisation has meeting its obligations.

FRAUD CONTROL STEPS

DFAT's arrangements require funding recipients to make ongoing efforts to protect their organisations from acts of fraud. DFAT's standard fraud clauses are included at the end of this Toolkit (see Annex 2). Please note that there are additional clauses included in arrangements that contribute to fraud minimisation, so funding recipients need to be aware of all requirements under their specific arrangements.

Although DFAT arrangements require funding recipients to conduct a fraud risk assessment and to develop a fraud control strategy, funding recipients have flexibility to adopt their own methods for managing fraud risks, provided they are appropriate to prevent, detect and correct fraud on DFAT. There are five (5) basic steps of fraud control that your organisation should implement:

Step 1
Conduct a Fraud Risk Assessment

Step 2
Develop a Fraud Control Strategy

Step 3
Implement, Test and Review Controls

Step 4
Report Fraud

Step 5
Correct and investigate

STEP 1 | CONDUCT A FRAUD RISK ASSESSMENT

Fraud risk assessments help organisations systematically identify fraud risks. Your organisation should conduct a general fraud risk assessment as part of its broader business improvement cycle.

Funding recipients must conduct a project specific fraud risk assessment and produce a fraud control strategy within one month of commencement of an arrangement with DFAT. A fraud risk assessment and strategy must be completed for each project your organisation is engaged by DFAT to complete.

Each fraud risk assessment and strategy must contain project specific fraud prevention, detection, investigation and reporting processes and procedures.

Identify Fraud Risks

The first step of a fraud risk assessment is to identify fraud risks as well as any weaknesses or deficiencies in internal and external controls.

When assessing fraud risks and identifying treatments your organisation should consider:

- the operating environment and associated risks
- possible methods for committing fraud,
- what might be attractive to a potential fraud perpetrator
- what fraud risks DFAT has identified (including in this Toolkit)
- what existing treatments are in place to prevent or detect fraud
- how current treatments might be circumvented.

DFAT's Key Fraud Risks

DFAT recognises that fraud is a category of crime that can affect any organisation regardless of its size or type. To assist funding recipients carry out fraud risk assessments, examples of key fraud risks that should be considered are listed in the table below. Also included in the table are some effective mitigation measures that can be used to address identified fraud risks. For more information on developing a strategy to address fraud and to implement controls, see Steps 2 and 3.

Please note the information included below is not exhaustive, appropriate fraud risks and controls for your project and organisation will depend on your specific circumstance and operating context.

Examples of Key Fraud Risks		
Theft and/or misuse of funds	Downstream sub-contractors not adhering to DFAT's or the funding recipient's policies and procedures	Falsified documents such as invoices being provided
DFAT contractors participate in bribery	Theft and/or misuse of assets	Facilitation payments are paid out of DFAT funds
Funds spent on items not allowed under the arrangement	Conflicts of interest i.e. contracts awarded to friends or family rather than seeking competitive quotes and maximising value	Collusion between downstream partners and external suppliers resulting in overspend

DFAT's Lessons Learned – How Funding recipients Can Prevent and Detect Fraud

1. **Keep records of all financial accounts:** Your financial systems must account for all expenditure against relevant budget lines. You must have the capacity to monitor and identify anomalies or discrepancies in spending.

2. **Ensure separation of duties:** To ensure accountability make sure that all processes and procedures provide sufficient segregation of duties, especially between the operation and financial areas. People who approve expenditure must not be in a position to benefit from that expenditure.

3. **Avoid Conflicts of Interest (COI):** When your organisation makes purchases or sub-grants activities you must ensure there is no conflict of interest in that process. A key mechanism to minimise this risk is having and publicising COI registers. Please refer to (Annex 6) for more information.

4. **Maintain arrangement compliance:** Your staff must understand the terms of your arrangement with DFAT. You must ensure that DFAT funds are only used for items that are clearly allowable under the arrangement in terms of both content and timing. Include regular checks on your organisation to ensure compliance.

5. **Guarantee value for money:** Train staff to ask 'Is this expenditure absolutely necessary to deliver the project?' and 'Would this expenditure stand up to public scrutiny?' If their answer is no to either question, then they must not expend taxpayer funds.

6. **Training of staff:** Ensure staff know their obligations under your organisation's arrangement with DFAT and are aware of DFAT's policies. Staff must be aware of what fraud is and how and where to report it.

7. **Ensure due diligence of sub-partners:** Ensure whatever downstream partner you are working with is a reputable entity and that they have the systems in place to manage funds.

8. **Active management of downstream partners:** Ongoing and active arrangement management is critical. It is too late to check after an activity is completed.

Identify Controls

Once fraud risks are identified, your organisation will be able to design specific detective, preventative and corrective control measures to treat and manage identified fraud risks.

Preventative controls

All DFAT funding recipients and their staff are required to prevent fraud on DFAT. Preventative strategies are the first line of defence and provide the most cost effective way of dealing with fraud.

Preventative controls manage the sources of the risk to decrease the likelihood of the risk occurring. For example training, procedures, contracts, agreements, segregating approvals and duties, governance arrangements, key performance indicators, communication strategies and awareness campaigns.

Detective Controls

All DFAT funding recipients and their staff are required to actively detect fraud and report any fraud identified**.** To do this you will need to monitor the progress of activities funded by DFAT.

> **Did you know?**
>
> **DFAT expects its funding recipients to actively look for and find fraud rather than passively waiting for fraud to be reported**

Detective mechanisms must be flexible, adaptable and regularly updated to meet changes in the fraud risk profile. Early detection is an essential element of fraud control.

Funding recipients must not rely solely on audits or downstream partners/members of the public reporting fraud, as, although these are good mechanisms, they are unlikely to detect all fraud. Your organisation must have mechanisms in place to validate that DFAT money has been spent in accordance with the arrangement. It is critical to have processes in place which enable your organisation to detect fraud quickly, as a delay in detection may lead to further fraud. Funding recipient staff play a key role in the detection of fraud and therefore require fraud awareness training so they are able to confidently identify the early warning signs of fraud and report appropriately (see Step 4).

> **Did you know?**
>
> **Statistically audits are not the most effective way to detect fraud. Our data shows that only a small portion of fraud is detected by delivery partner audits. Audits are a powerful tool but cannot be relied upon as a sole mechanism to detect fraud.**

Detective controls produce evidence that controls are functioning, or identifies new or emerging risks, or identifies issues that have occurred. For example regular reporting and testing, site visits, phone calls, photos, workshops, videos, validation checks, audits and reviews. DFAT arrangements typically require funding recipients to conduct an annual audit. DFAT's standard position is for this to be a 'compliance audit' tailored to the specific project/s (see Appendix 7).

Corrective controls

Corrective controls decrease the extent of the consequence once the risk event has occurred. For example a crisis management plan, insurance, increased monitoring.

STEP 2 | DEVELOP A FRAUD CONTROL STRATEGY

A fraud control strategy articulates how an organisation will manage fraud risks. A fraud control strategy may include:

- a summary of identified fraud risks
- treatment strategies and controls designed to manage identified risks and vulnerabilities
- Information on how to implement fraud control arrangements within the organisational context
- training and awareness strategies designed to meet the organisations needs/obligations
- a description of the organisation's method of collecting, analysing and reporting fraud
- protocols for handling fraud incidents
- an outline of key responsibilities/individuals in the fraud space.

Did you know?

Policies and processes are important fraud controls but are not efficient if organisations do not have checks to ensure that people are complying. A strong governance framework supports your internal processes and sets the standard for fraud control within your organisation.

Fraud doesn't happen in isolation. It is usually the result of a failure or lack of governance or adherence to procedures. Therefore, sound governance and oversight are critical to fraud prevention.

To prevent and detect fraud, your organisation's fraud control strategy should include strategies at an organisational level, such as governance arrangements, as well as strategies tailored at the country and project levels. To ensure the controls and corrective measures identified as part of the fraud risk assessment are implemented and to adhere to DFAT's fraud control obligations, a strong governance framework is required. By addressing any shortcomings in your own governance framework, you are ensuring that fraud risks will be more readily detected and reported.

Governance

While governance arrangements may vary from organisation to organisation, in principle they are a combination of processes and structures that inform, direct and manage day to day business activities, to achieve objectives.

The illustration of good fraud risk governance below shows that integrity, ethics and conduct surround all activities. An oversight body, such as a board of directors, can play an important role in ensuring effective governance. Fraud risk management functions including fraud risk assessments are undertaken to identify fraud risk and to evaluate and prescribe fraud control mechanisms. Internal controls, which include any processes or systems used to minimise fraud, are at the centre of fraud risk governance because a strong control environment is integral to fraud control.

1. Integrity, Ethics & Conduct

2. Oversight

3. Fraud Risk Management

4. Internal Control

How Strong is your Governance Framework?

When assessing the strength of your organisation's approach to fraud risk governance, you should consider whether the governance framework in place in your organisation is able to:

- convey the expectations of oversight committees, such as the role of the board of directors
- ensure fraud risk assessments are conducted regularly to identify new or emerging fraud risks
- identify and implement prevention techniques that mitigate the potential impact of fraud
- identify and implement detection techniques to uncover acts of fraud, should prevention techniques fail
- implement reporting processes and
- identify and implement correction techniques to enable your organisation to respond to fraud effectively and efficiently update your fraud control strategy.

To assist the self-assessment process, the checklist located at Annex 3 can be used to self-assess your compliance.

Did you know?

If your organisation has many DFAT funded projects in similar countries or regions, your organisation could develop an overarching fraud control strategy to address homogeneous fraud risks. However, this high-level strategy must be complemented by project level assessments and fraud control strategies aimed at addressing project/program specific risks.

STEP 3 | IMPLEMENT, TEST AND REVIEW CONTROLS

Once a project level fraud risk assessment and strategy has been completed, your organisation should implement the identified controls to remove the opportunity and motivation for fraud.

Mechanisms need to be developed to monitor the implementation and to test the effectiveness of controls. The governance framework outlined in the fraud control strategy should designate who is responsible for the implementation of identified controls. An oversight protocol for the implementation and testing of controls should also be outlined.

Did you know?

Trust is not a control. Mechanisms able to detect fraud must be in place. Trusted employees' circumstances can change, giving them motivation to commit fraud should the opportunity arise.

Awareness and Training

Funding recipients and their staff play a significant role in the detection of fraud.

Without specific fraud awareness training these individuals may not understand your organisation's fraud control strategy, the controls that are designed to minimise fraud, how to recognise fraud and where to report it. All staff should be made aware that preventing, detecting and reporting fraud are part of their normal responsibilities.

Training could include:

- information on typical indicators of fraud
- information on the functionality of your organisation's fraud strategy; for example, an overview of fraud prevention, detection, correction and reporting mechanisms
- an overview of internal policies which contribute to fraud risk reduction such as your organisation's ethics policy or code of conduct.

Funding recipients should ensure records are retained of staff who have completed training.

Fraud Control Strategy Review

Funding recipients must review and update their fraud risk assessments and fraud control strategies regularly (6 monthly at a minimum) and in response to a fraud event or any other change the risk profile.

STEP 4 | REPORT FRAUD

Reporting Culture

DFAT looks upon self-reported incidents of non-compliance more favourably than non-reported incidents. DFAT knows that fraud can occur in the locations where we operate. Our focus is on preventing fraud where possible and ensuring that your organisation is well equipped to detect and manage fraud. DFAT does not penalise organisations for reporting fraud. DFAT also checks programs that, in comparison to their level of funding, have under-reported incidents of fraud.

> **Did you know?**
> **DFAT does not require cases of stolen portable and handheld devices (such as mobile phones, iPads and laptops) to be reported as fraud. If the theft isn't specifically targeting DFAT property or information, such incidents should be dealt with by reporting the theft to your DFAT project/program manager and repaying an agreed amount to the program or replacing the item.**

Reporting Fraud to DFAT

Funding recipients must report any suspected or real incidents of fraud **within five (5) business days** at which point DFAT can help your organisation correct the situation. A template of the 'Fraud Referral Form' is located here. Any suspected or real incidents of fraud, aside from passport fraud, must be reported to the Fraud Control Section and to your arrangement/activity manager.

Public Interest Disclosure

Public officials or persons deemed public officials, including funding recipients, can report instances of suspected internal fraud under the *Public Interest Disclosure Act 2013* to an Authorised Officer.

The *Public Interest Disclosure Act (2013)* protects the persons making the allegation from reprisal. Disclosures may be made:

- In writing: For Authorised Officer Only | Public Interest Disclosure | Management and Corporate Strategy Section | Department of Foreign Affairs and Trade | R.G. Casey Building, John McEwen Crescent | BARTON | ACT | 0221
- Email: PID@dfat.gov.au
- Phone: (02) 6178 4321
- Email: fraud@dfat.gov.au

Reporting Terrorism Financing

All concerns and suspicions relating to the diversion of public or private funds, including DFAT funds, to terrorists should be provided to:

- The National Security Hotline – 1800 123 400
- DFAT Sanctions Section – sanctions@dfat.gov.au
- Transnational Crime Section – transnational.crime@dfat.gov.au

Reporting Passport Fraud

Passport fraud is generally dealt with under the *Australian Passport Act (2005)*. Report any suspected or real incidents of passport fraud to Australian Passport Office.

- Phone: 131 232
- Email: passports.fraud@dfat.gov.au

> **Do not wait to report an incident of fraud to DFAT until you have more information. Your arrangement with DFAT requires you to report fraud to DFAT within 5 business days of your organisation being notified of or identifying the potential fraud.**

STEP 5 | INVESTIGATE AND CORRECT FRAUD

For all instances of attempted, alleged, suspected or detected fraud, DFAT requires an investigation of the matter. Your organisation needs to investigate detected, suspected or attempted fraud in accordance with the principles set out in the Australian Government Investigation Standards (AGIS) and the laws of the jurisdiction in which the fraud incident occurred. The fraud case manager checklist (Annex 4) provides guidance for individuals conducting investigations and outlines how fraud cases should be managed.

DFAT oversees (and may direct) the management of fraud allegations and investigations. If fraud is identified, then DFAT will:

- apply administrative or contractual penalties
- seek prosecution of offenders and
- seek the recovery of fraud losses.

Investigative Procedures

Your organisation must have investigative procedures in place that align with the requirements of AGIS.

Qualifications of Staff

Your arrangement will specify the qualifications required of investigators. Typically, the DFAT arrangements state that investigators must have the minimum requirements outlined in AGIS. AGIS requires investigations staff to have at a minimum the following qualifications:

- **investigator:** Certificate IV in Government (Investigation), or its equivalent,
- **staff involved in the coordination and supervision of investigations**: Diploma of Government (Investigation), or equivalent.

Whether your organisation conducts an investigation or appoints an investigator to conduct an investigation, the person conducting the investigation must possess the minimum qualifications specified in the Australian Government Investigation Standards or an equivalent acceptable to DFAT. Equivalent qualifications deemed acceptable to DFAT include legal, audit and alternate formal investigations qualifications.

Contact fraud@dfat.gov.au for more advice on acceptable qualifications or to seek formal approval for individuals to conduct investigations if their qualifications are different to those listed above.

Reporting to Police or Government Agencies

To resolve incidents of fraud, the funding recipient will be required to report fraud to an appropriate law enforcement agency. Before doing this, funding recipients must consider if reporting the incident:

- could compromise the safety of a person's life or
- could significantly impact on them to an extent which would result in undue hardship or
- could result in a disproportionate response to the circumstances of the fraud (taking into account remedial actions already taken by your organisation).

If the above factors exist, please seek an exemption from police reporting from FCS by sending an email to fraud@dfat.gov.au.

When cases are reported to local authorities, DFAT requires details of police reporting such as the date reported, a copy of the police report, reference numbers and results of the police investigation (where possible).

Dealing with Non-Compliance

Where non-compliance rather than fraud is identified, it must be dealt with in accordance with contractual procedures, promptly and proportionately to the wrongdoing identified.

Learning From Past Incidences of Fraud

Funding recipients are expected to use lessons learnt to inform future business practices and to control for fraud. By learning from past experiences and each other, DFAT and its suppliers can work together to better manage fraud and corruption.

Where fraud risks eventuate (a fraud occurs), funding recipients must evaluate the effectiveness of existing fraud risk treatments so that lessons are learnt and corresponding changes made to the fraud risk assessment, training and the fraud control strategy.

Did you know?
Exemption from reporting to local authorities/police can be granted by the Director of FCS via fraud@dfat.gov.au

ANNEX 1: THE DEFINITIONS

Arrangement

- Collectively refers to the many types of arrangements DFAT enters into under different names e.g. contracts, agreements, arrangements, memorandums of understanding (MOU) etc.

Fraud

Fraud against the Commonwealth means **dishonestly obtaining a benefit, or causing a loss, by deception or other means.** It includes:

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

People usually associate fraud with monetary or material benefits. Gains are not only about monetary or material benefits. For example, a person can receive benefits by giving away

Corruption

sensitive or classified information.

Corruption is a type of fraud. Corruption is a misuse of entrusted power for private gain. The Commonwealth defines corruption as:

- Conduct that involves, or that is engaged in for the purpose of, the staff member abusing his or her office as a staff member of the agency.

- Conduct that perverts, or that is engaged in for the purpose of perverting, the course of justice.
- Conduct that, having regard to the duties and powers of the staff member as a staff member of the agency, involves, or is engaged in for the purpose of, corruption of any other kind.

Fraud Risk Assessment

A **fraud risk assessment** identifies fraud risks and corresponding controls to minimise or mitigate the identified risks.

Fraud Control Strategy

A **fraud control strategy** the plan for how fraud will be managed or controlled in an organisation or program.

Collusion

Collusion is a deceitful agreement or compact between two or more persons or organisations, aimed at defrauding a third party. Collusion against DFAT could involve DFAT officers, funding recipients and/or other parties.

Internal Fraud

Internal Fraud is fraud **committed by a DFAT officer**, and is generally dealt with under the *Public Services Act 1999.* For locally engaged staff (LES) at posts, the LES Code of Conduct applies in conjunction with local employment law. Corruption is a type of internal fraud.

External Fraud

External Fraud is fraud **committed by a party external to the Commonwealth**, for example, funding recipient entrusted with the use of public funds. It can be dealt with under a range of civil or criminal provision, contract clauses, or other mechanisms depending on the location of the incident.

Passport Fraud

Passport Fraud is, for example, **making false declarations in the application**. Passport fraud is dealt with under the *Australian Passports Act 2005.*

ANNEX 2: STANDARD FRAUD CLAUSES

DFAT communicates and enforces its expectations relating to fraud and corruption control via arrangement provisions with its funding recipients. DFAT's arrangements typically include standard fraud clauses which detail the responsibilities of DFAT's funding recipients. The standard fraud clauses place the obligation on funding recipients to investigate allegations and suspected fraud cases in the Australian aid program. Contract and grant arrangement obligations, on a proportional risk basis, are likely to require program funding recipients to:

- Ensure that the partner and/or its personnel do not engage in any fraud. Fraud must be actively prevented and detected, including by the partners personnel.
- Adhere to the relevant conflict of interest and confidentiality clauses.
- Ensure that the partner or its personnel do not make or cause to be made, receive or seek to receive any offer, gift, payment or benefit of any kind, which could be construed as an illegal or corrupt act.
- **Within one month of Project Start Date**: conduct a fraud risk assessment and produce a fraud control strategy in compliance with the Commonwealth Fraud Control Framework available at www.ag.gov.au.
- Ensure risk assessments and strategies contain appropriate fraud prevention, detection, investigation and reporting processes and procedures.
- Ensure that personnel are responsible and accountable to the funding recipient for preventing and reporting fraud as part of their routine responsibilities. This includes reporting potential fraud matters **within five (5) business days.** A template of the 'Fraud Referral Form' is located here.
- Respond **within five (5) business days** to any further requests for information by DFAT

- Investigate any fraud and bear the cost of the investigation in accordance with any directions or standards required by DFAT.
- Have access to an investigator (internal or appointed) that possesses the minimum qualifications specified in the Australian Government Investigation Standards or an equivalent agreed to by DFAT.
- Provide reasonable assistance and bear associated costs should DFAT choose to appoint its own investigator in accordance with the contract terms.
- Report any suspected offenders identified as part of the investigation to the appropriate law enforcement agencies, unless the Director of DFAT- Fraud Control Section agrees otherwise in writing.

These standard clauses also require commercial and NGO partners to repay funds or replace assets lost to fraud including taking recovery action in accordance with recovery procedures (including civil litigation) available in the partner country. This applies if the fraud was committed by the organisation or an employee of the organisation, a funding recipient or subcontractor of the organisation, or employees of funding recipients or subcontractors of the organisation. DFAT uses these clauses to recover funds where appropriate. Other arrangements cover partner governments and multilateral organisations.

Additionally, as part of DFAT's due diligence checks on DFAT's major funding recipients, DFAT arrangements may require funding recipients to present a code of conduct, fraud control policy and anti-corruption/bribery policy to ensure their compliance. Funding recipients are also contractually required to act in accordance with the Commonwealth Procurement Rules, of which due diligence assessments are a component.

ANNEX 3: SELF-ASSESSMENT CHECKLIST

This checklist has been developed to assist funding recipients understand and meet DFAT's fraud control obligations. The checklist is designed to showcase best practice procedures/processes as well as to outline DFAT's mandatory requirements.

Stage 1 of this checklist focuses on the organisational level, Stage 2 considers fraud control at an individual project level, and Stage 3 is designed to assess the fraud control mechanisms your organisation has in place to prevent, detect and correct fraud carried out by downstream partners.

STAGE 1: ORGANISATIONAL LEVEL

Your organisation should conduct a general fraud risk assessment as part of your organisation's broader business improvement cycle.

Best Practice	Mandatory	1.1 Organisation Procedure/Policy Specifics	Y	N	N/A
●		Your organisation has conducted a general risk assessment			
●		Your organisation has a fraud control strategy in place			
●		The fraud control strategy/policy is current			
●		Your fraud control strategy/policy stipulates how your organisation should assess the risk of fraud to your organisation			
●		Your fraud control strategy/policy addresses corruption, bribery, facilitation payments, training, mechanisms for internal and external reporting of fraud and whistle-blowing processes			
●		You have an employee code of conduct and ethics or you have other policies that address fraud, corruption and ethics in your organisation			
●		A strong policy position is in place ensuring that your organisation on the whole: • is open and honest • has developed insight into the causes and consequences of previous problems • demonstrated that they have addressed previous problems • complied with all contractual conditions • complied with DFAT reporting requirements, including a detailed audit of financial records • has strong governance arrangements in place.			

STAGE 2: PROJECT LEVEL

Stage 2 is split into three sections. Prevention, detection and correction. Examples of controls are included at the end of each subsection.

Best Practice	Mandatory	2.1 Fraud Prevention Considerations	Y	N	N/A
	●	Your organisation has conducted a fraud risk assessment and produced a fraud control strategy **within one month of the project start date**			
	●	The fraud control strategy has been communicated to staff			
	●	Approach to fraud risk assessment has been established, including its oversight			
	●	An oversight protocol for the implementation and testing of controls has been outlined			
	●	Your organisation includes fraud and anti-corruption clauses in its contracts, MOUs, other types of arrangements with your partner organisations			
	●	Formal mandatory training is provided on fraud and anti-corruption			
	●	Refresher training is mandatory on a regular basis			
	●	Records of staff who have completed training are kept			
	●	Staff understand and are trained in applying the 'Value for Money' principles			
	●	Policies and procedures are in place to guide decision-making			
	●	Conflict of interest policy and process is clear for internal and external persons			
	●	Service delivery is substantiated before invoices are paid			
	●	Fraud risk assessments and fraud control strategies are reviewed and updated on a 6 monthly basis to ensure risks and treatments are appropriate			
	●	Checks of the identities of employees, suppliers and downstream partners have been carried out			
	●	Responsibilities and performance expectations are clearly articulated			
	●	Compliance strategies have been communicated to stakeholders			
	●	Communication strategies articulate what compliance looks like			
	●	An early-intervention and compliance plan is in place to respond to any issues			
	●	Funding is traceable			
	●	Separation of duties occurs where applicable			
	●	Official information or security classified information is handled in compliance with all relevant security requirements specified in the Commonwealth Protective Security Policy Framework			

Examples of Preventative Controls

The list of controls is not exhaustive; rather it is designed to provide examples of suitable prevention mechanisms

Physical and information security controls	ICT security and access control systems and policy	Policies and procedures
Ethics programs	Defined roles and responsibilities	Conflict of interest register
Regular documented fraud risk assessment	Regular awareness training	Code of conduct affirmation
Police checks	Separation of duties and approvals	Governance arrangements, including board oversight
Key performance indicators	Fraud risk assessments	Secure storage of equipment

Examples where duties should be separated could include:

- Accounts receivable, cash application and billing

- Vendor set up and payment preparation

- Disbursement approval and recording

- Procurement, receiving and payment

- Receiving and recording cash

- Disbursing and reconciling petty cash

- Billing and accounts receivable credits

- Electronic banking payment initiation and release

- Banking transaction process and bank reconciliation preparation

- Changes to vendor bank details requiring two part signoff

In practice, the level of segregation of duties applicable to your organisation will depend on the size of the local finance team and the amount of funding your organisation receives.

Best Practice	Mandatory	**2.2 Fraud Detection Considerations**	Y	N	N/A
	●	Funding is tracked			
	●	Assurance activities are conducted to validate expenditure			
	●	Data is collected to inform compliance with DFAT arrangements			
●		Critical fields are analysed in the records system (e.g. a database)			
●		Internal or external persons undertake evaluations or reviews			
	●	Information is recorded in the records system			
●		Data is compared to similar benchmarked programs to provide a comparison			
	●	Quality of outputs is measured (site visits, photo evidence, desktop reviews)			
	●	The format of the financial acquittal complies with DFAT's requirements			
	●	Action is taken if the acquittal is inadequate			
●		Where possible, funds are acquitted progressively			
	●	Acquittals are checked and signed off by the authorised person			
	●	A mechanism for staff to report fraud to your organisation exists			
	●	A mechanism for the public to report fraud to your organisation exists			
	●	Staff and members of the public can report fraud anonymously to your organisation			
	●	Internal reviews of compliance with internal policies and DFAT's arrangement are conducted regularly			

Examples of Detective Controls

The list of controls is not exhaustive; rather it is designed to provide examples of suitable detection mechanisms

Evaluations and quality assurance checks (both desktop and at site)	Maintain an asset register and conduct an annual stocktake of assets	Ensure access to systems done so through unique identifiers so work areas can trace who entered data
Whistleblowing Processes	Internal and External Audits	Inspections and Surveys
Ensure an audit trail (data log) of changes made to the IT system, including when changes were made and by which user	Monitoring and acquitting of expenditure through monthly reconciliation of invoices/statements by delegate	Build capacity to allow work areas to identify data or patterns which may indicate the emergence of a fraud risk
Conduct random process checks regularly	ICT access logs are maintained and reviewed periodically	Review any entitlement claims, such as travel claims
Maintain vehicle logs, listing the dates, times, mileage or odometer readings, purpose of the trip, and name of the officer using the vehicle	Manage audit of expense reports, credit card charges, and telephone bills periodically to determine whether charges are appropriate	Separate handling (receipt and deposit) functions from record keeping functions (recording transactions and reconciling accounts)
Maintain an equipment list and periodically complete an inventory	Conduct audits of personal leave and hours worked if needed	Conduct checks on claims in job application submissions
Conduct referee checks	Key Performance Indicators	Verify education qualifications

It is important to consider including alerts where actions are undertaken in a system that may pose a fraud risk e.g.

→ A number of changes made to specific fields in a short timeframe

→ Changes made to certain fields after data has been entered

→ High payment requests by certain users

→ A lack of data entered or evidence provided

Best Practice	Mandatory	2.3 Fraud Investigation and Correction Considerations	Y	N	N/A
	●	You maintain an internal database on alleged, suspected or detected fraud reports and progress of investigations			
●		Senior management receive regular updates on fraud reports and investigations			
	●	You have access to investigators qualified under AGIS			
	●	Contractual obligations around reporting fraud to DFAT and how this is done are communicated to staff. This includes staff understanding that potential fraud matters must be reported to DFAT **within five (5) business days.**			
	●	A procedure outlining how to report fraud to law enforcement agencies and how to seek an exemption from this requirement has been developed			
	●	Contractual obligations regarding reporting fraud to law enforcement agencies have been communicated to staff			
	●	You have implemented and trained relevant staff in investigative procedures that comply with the principles of AGIS			
	●	Reporting on progress of investigations is performed in accordance with your arrangement			
●		Findings from evaluations are used to make policy or contractual changes			
	●	Findings of non-compliance or fraud are shared with other areas and corrections made to prevent reoccurrence			
	●	Staff understand what can and can't be charged to DFAT in accordance with your contract			
●		The responses to non-compliance directly respond to the level of risk and the significance of the breach (e.g. you might deal with a small, low-risk problem via an email or telephone discussions, and a large problem involving more money with more frequent attention and a more hands-on approach, such as site visits).			
	●	DFAT is kept abreast of incidences of non-compliance via monthly follow-up meetings			

Examples of Corrective Controls

The list of controls is not exhaustive; rather it is designed to provide examples of suitable correction mechanisms

Crisis management plan	Insurance	Increased monitoring
Formal evaluations	Training and awareness	Implementing controls
Re-conducting fraud risk assessment	Recovery of funds	Other measures imposed by DFAT

STAGE 3 DOWNSTREAM SUPPLIER LEVEL

Best Practice	Mandatory	**3.1 Downstream Supplier Checklist** Use this checklist to review contractual arrangements with downstream subcontractors through a fraud lens.	Y	N	N/A
	●	A fraud risk assessment and fraud control strategy have been completed			
●		Goals are precise in the arrangement to allow for later evaluation			
●		Relevant training has been identified and delivered			
	●	Standard contract or arrangement clauses have been included, including fraud and anti-corruption clauses			
	●	It is stipulated that any variation to the arrangement must be made in writing			
	●	Responsibilities and performance expectations are clearly articulated			
	●	Programs undergo regular reviews and are adjusted to remain relevant			
●		The funding recipient's fraud control strategy has been approved			
	●	Instances of non-compliance are always dealt with and escalated appropriately if funding recipients fail to deliver on critical activities or milestones or act inappropriately			
	●	Contracts or arrangements are varied to address evaluations, non-compliance or fraud risks			
	●	Financial acquittal policy is available to funding recipients			
	●	Acquittal policy linked to the level of financial risk			
	●	Key performance indicators have been developed, and they are specific, measurable, achievable, realistic and with timeframes			
	●	Formal evaluation has been designed, including key questions			
	●	Required data has been identified to inform future evaluations			
	●	Checks are routinely and randomly carried-out in accordance with DFAT arrangements to validate service delivery and claims for payment			
	●	Risk assessments are conducted on all downstream partners			
	●	Risk based and proportionate due diligence is conducted on all downstream suppliers including individual/organisation identity checks.			
	●	Organisations are crosschecked against The Asian Development Bank's Sanction List, World Bank Listing of Ineligible Firms and Individuals, the Consolidated List and the Australian National Security Listed Terrorist Organisations List to find out if a person or entity is subject to sanctions or have been formally declared as being involved in terrorism			

NOTE: The level of management of downstream partners required is context specific. The level of oversight your organisation has over your downstream partner's operations should be proportionate to the identified level of risk. When assessing risk in this context it is important to consider:
- **the risk posed by the partner** (i.e. unknown partners will require a higher level of intervention),
- **the level of project specific risk** (i.e. higher project risk will require more involvement) and
- **the value of the arrangement or project** (i.e. higher value projects will require more controls).

ANNEX 4: FRAUD CASE MANAGER CHECKLIST

Best Practice	Mandatory	**4.1 Fraud case manager obligations** Use this checklist if you are managing a fraud case.	Y	N	N/A
		Referral of fraud			
	●	Ensure that the 'Fraud Referral form' is emailed to FCS at fraud@dfat.gov.au within 5 business days of an alleged, suspected or detected fraud			
	●	Ensure relevant senior managers in your organisation are advised and your relationship or program manager at DFAT is notified of the fraud			
	●	Ensure any details not known or provided on the initial form are updated and provided to FCS once available.			
	●	Do not discuss or disclose information to anyone (other than senior managers in your organisation) before checking with FCS.			
	●	Maintain confidentiality. Information about persons reporting fraud is NOT to be disclosed.			
		Management of Referrals			
	●	Respond in a timely manner to requests for information and/or action from FCS.			
	●	Familiarise yourself with the relevant contracts/arrangements with downstream suppliers when a fraud is attempted, alleged, suspected or detected in a particular program.			
	●	Check whether the alleged behaviour was permitted under the program/arrangement/guidelines or by DFAT in some other way (i.e. though advising the Funding Recipient that they could do something)			
		Management of Fraud Cases *Usually under the arrangement cases will be investigated by the Funding Recipient*			
	●	Liaise with any third parties involved in the attempted, alleged, suspected or detected external fraud (after reporting to FCS, and at the direction of FCS).			
	●	Ensure records are kept to document the matter.			
	●	Provide FCS with a progress report on the fraud matter every month, including a nil report where no progress has been made.			
	●	Ensure that funds/assets subject to misappropriation are recovered in full.			
	●	With guidance from FCS, ensure that appropriate penalties are sought.			
	●	Provide FCS with relevant case numbers/reports issued by local authorities.			
	●	Advise FCS of any disciplinary action taken as a result of the investigation. Actions may include employment termination/resignation or legal prosecution.			
	●	Advise FCS of any mitigation strategies implemented to prevent reoccurrence of the fraud.			
	●	When all zero tolerance conditions have been met (or exemptions granted) recommend to FCS that the case be closed.			

ANNEX 5: BRIBERY AND FACILITATION PAYMENT FACT SHEET

WHAT IS BRIBERY?

Bribery is the promise or delivery of a benefit in order to influence the receiver's behaviour. Usually the behaviour expected of the person receiving the bribe is illegal or unethical in nature and would not be something they would usually do. However the return behaviour itself does not have to be illegal or unethical in order for it to fall within the definition of bribery. Bribing or attempting to bribe a foreign public official is a serious crime. Australian companies or individuals that bribe an official in a foreign country can be prosecuted under Australian law and the laws of foreign countries. All incidents of suspected bribery of foreign officials must be reported to the Transnational Crime Section:

- transnational.crime@dfat.gov.au

WHAT ARE FACILITATION PAYMENTS?

Facilitation payments are low-value payments designed to speed up routine government actions. These are sometimes referred to as 'grease payments'.

Facilitation payments create incentives for public officials to slow down processes and create obstructions. Facilitation payments leave organisations open to exploitation and reputational risks. A growing body of research and experiences demonstrate that business can achieve net gains by refusing to make facilitation payments.

Facilitation payments have a corrosive effect, particularly on sustainable economic development and the rule of law. Regardless of their value, such payments amount to public officials personally benefitting from providing a public service. They undermine local laws and entrench corrupt practices.

WHAT IS DFAT'S POLICY ON FACILITATION PAYMENTS?

The use of facilitation payments could link the success of Australian endeavours, including the Australian aid program, to corrupt officials. It can create an impression that Australia endorses corrupt behaviour and undermines our efforts to promote good governance.

Therefore DFAT prohibits the use of facilitation payments with Commonwealth funds, by its staff and partners unless there is a threat to the health or safety of an individual.

The Australian Government strongly discourages Australian businesses and individuals from paying facilitation payments.

WHAT CAN I DO TO AVOID REQUESTS FOR FACILITATION PAYMENTS?

Develop a strategy to avoid requests for facilitation payments, and plan for how to resist requests when they may arise.

- Know the local laws in relation to facilitation payments. This will make it easier to resist paying a facilitation payment if one is requested.
- Know the process and costs before applying for authorisations and permits. If possible, obtain official written confirmation that all required information and documentation is in order.
- When paying fees, make it clear that you will require an official receipt that identifies the amount paid, what the payment is for, when it was made and to whom it was made.

- Avoid last minute applications. Requests for facilitation payments are often made to expedite approval processes. Avoiding time pressure makes resistance to facilitation payments easier.

WHAT SHOULD I DO IF I AM ASKED FOR A FACILITATION PAYMENT?

- Question the legitimacy of the request.
- Explain to the person requesting the payment that you do not feel you are required to make the payment as all your paperwork is in order. This is where having a solid understanding of the process will work to your advantage.
- Explain that making a facilitation payment is against DFAT's policy and that you are not authorised to make facilitation payments from DFAT's funds.
- Point out that facilitation payments are against local laws, if this is the case.
- Raise with senior management at post who can raise with host governments if appropriate.

WHAT IF THE REQUEST FOR A FACILITATION PAYMENT IS ASSOCIATED WITH THREATS TO SAFETY OR OF VIOLENCE?

In certain circumstances, not paying a facilitation payment can create a threat to health or safety. In such a case, the payment should be made, documented and reported to DFAT as soon as possible. If asked for a facilitation payment, only resist making the payment if you feel safe. If the request is accompanied by threats, make the payment and record as much detail as you can when in a safe location. Then report the matter to your manager and the Fraud Control Section as soon as possible after the event. The record should include:

- The name of the individual who requested the payment.
- The date and time the request was made and how much was requested.
- The steps you took to resist making the facilitation.
- Nature of any threats, intimidation or violence that was involved.
- Any other relevant detail.

Never refuse to make a payment if you are faced with a threat, or believe there is a threat to your safety. The safety of our partners is of upmost importance to us.

WHO SHOULD I ASK MORE QUESTIONS ABOUT FACILITATION PAYMENTS?

If you have questions about facilitation payments, please contact the Fraud Control Section at fraud@dfat.gov.au.

If you have questions about foreign bribery, please contact the Transnational Crime Section at transnational.crime@dfat.gov.au.

ANNEX 6: CONFLICT OF INTEREST FACT SHEET

WHAT IS A CONFLICT OF INTEREST?

A conflict of interest is a situation where an individual or an organisation has multiple interests, one of which may improperly influence the performance of that individual's or that organisation's duties and responsibilities. A conflict of interest creates the appearance that an individual's or an organisation's objective judgement is likely to be compromised, biased. Conflicts of interest can be real, apparent or potential:

> **Real:** where a direct conflict exists between current official duties and other interests;
> **Apparent:** where it appears or could be perceived that other interests are improperly influencing the performance of official duties – whether or not that is actually the case;
> **Potential:** where other interests are not but could come into direct conflict with official duties.

Conflicts of interest can arise in relation to financial interests such as shareholdings, employment opportunities, real estate and trusts, as well as non-financial interests such as affiliations, associations and reputational interests that can conflict with duties and responsibilities. In addition, a conflict can include not only the interests of individual staff and contractors, but also the interests of their relatives (such as spouses, siblings or dependants) and the interests of their business partners or associates. Conflicts of interest can happen without anyone being at fault. However, it is vital that conflicts of interest are disclosed and managed effectively so that your organisation performs its duties in a fair, transparent and unbiased way.

WHY DO I NEED TO BE AWARE OF CONFLICTS OF INTEREST?

All funding recipients have an important duty to uphold and promote the positive reputation of Australia, the Government and the department. This reputation can be compromised by conflicts of interest. For this reason, there are direct and indirect references to conflicts of interest (including obligations and sanctions) in the contractual arrangements between the department and its partners.

WHAT DO I NEED TO DO?

The onus is on funding recipients to be alert to any conflicts of interest in connection with their duties and responsibilities; to disclose any such conflicts to the department; and to take reasonable steps to avoid any situation where their other interests conflict or could be perceived to conflict with their duties and responsibilities.

Funding recipient staff or representatives must regularly assess whether they have any conflicts of interest. Make sure staff ask themselves: could my personal or private interests or other interests of my organisation be perceived to improperly influence the decisions I make, the actions I take or the advice I provide in connection with my duties and responsibilities? If the answer is 'yes', then they must immediately disclose these interests and any circumstances which may be perceived as involving a conflict of interest to the department. As well as disclosing any conflicts of interest to the department, all funding recipient staff must also take reasonable steps to avoid situations where their other interests conflict (or could be perceived to conflict) with their duties and responsibilities. Funding recipients have

specific responsibilities and obligations outlined in their contractual or grant arrangements with the department. As a general rule, to enter into an arrangement with DFAT, funding recipients and their staff are required to:

- disclose the details of any conflicts of interest; or
- declare that no conflicts of interest exist – or are likely to arise – in the performance of that funding recipient's obligations under that arrangement.

In addition, funding recipients are required to use their best endeavours to ensure that no conflicts of interest arise in relation to the performance of that arrangement. If a conflict does arise, funding recipients are required to immediately notify DFAT in writing.

WHAT SITUATIONS MIGHT PRESENT A CONFLICT OF INTEREST?

The principle test is whether the circumstances create the appearance that an individual's or staff's objective judgement is likely to be compromised, biased or partial. See below for some common situations that might present conflicts of interest:

- A staff member is involved in a procurement tender process. The staff member has a sibling employed with a company bidding for work related to the tender.
- An employee of the funding recipient is appointed to a DFAT scholarship selection panel. The employee works with, or knows, one of the applicants personally.
- An NGO has received a grant from DFAT. The NGO is running a procurement tender process for the expenditure of some of the grant money. An employee of the NGO has shares in a company that is bidding for the tender.
- A funding recipient is managing an infrastructure project on behalf of DFAT. A staff member of the funding recipient is running a procurement tender process as part of the project. The staff member has a cousin employed with a company bidding for work related to the tender.
- An NGO is contracted by DFAT to assess grant applications. An employee of the NGO belongs to an association or a community group that has applied for a grant.
- A DFAT employee is involved in an aid project. The employee volunteers for a NGO that is bidding for work related to that project.
- A funding recipient is managing an aid project on behalf of DFAT. An allegation of fraud is made in relation to the project and the partner organisation. The partner organisation appoints its own employees to investigate the fraud allegation.

For any queries about conflicts of interest, please contact the Fraud Control Section at fraud@dfat.gov.au.

ANNEX 7: DFAT STANDARD AUDIT

DFAT arrangements typically require funding recipients to conduct an annual audit. DFAT's standard position is for this to be a 'compliance audit' tailored to the specific project/s. The Terms of Reference (TOR) are to be created in consultation with DFAT Agreement Manager.

Types of Audits

Auditing Standards
International standards on Auditing(ISA) by the International Federation of Accountants (IFAC)

COMPLIANCE AUDIT	FINANCIAL STATEMENT AUDIT	PERFORMANCE AUDIT	INFORMATION SYSTEMS (IT) AUDIT	INTERNAL CONTROL AUDIT
The objective of a compliance audit is to express a conclusion on whether an entity has complied in all material respects, with requirements as outlined in criteria. A compliance audit is different from an external audit, as the auditor is not forming an opinion on the financial report, but on the specified criteria outlined by the client. It is commonly used to verify the compliance of rules including legislation, regulation and contractual and regulatory requirements.	Provides independent assurance that management has presented a true and fair view of the financial performance and position.	Provides verification that resources are being used in the best possible manner to fulfil the aim and objective of the organisation.	Provides an evaluation of IT systems paying particular attention to data reliability	Assessing the effectiveness of controls in preventing and mitigating the possible risk of misstatement.
Examples: - Contractual compliance which can be a broad review or tailored approach to address specific areas/risks (this could include expenditure eligibility under contract etc.). - Business process weaknesses - Assessment of adherence with policy and procedures, - Internal governance structures	Examples: - Transactional level testing (supplier expenses etc.) - Systems and processes (including IT systems) - Control weaknesses - Accuracy and appropriation of amounts Financial Management System (FMS) and record keeping	Examples: - Procurement process achieved overall value for money - Deliverables achieved overall objective and were within budget	Examples: - Payment run assessment - Vendor change management - Super user access/activities	Examples: - Grant acquittals - Reconciliations Supplier payment and payment runs - Vendor change management - Control effectiveness or weaknesses

ANNEX 8: MINIMISING FRAUD IN CASH TRANSACTIONS

In some countries, electronic transactions are the exception and cash (including cash cheques) is widely used. Cash transactions are a higher fraud risk than electronic transactions because, where is it misappropriated, it is much harder to trace. Consequently cash should only be used where there is no other option. In these circumstances, controls must be implemented to minimise potential fraud. The controls need to be tailored to the local risks and operating framework of the organisation.

Examples of Minimising Fraud in Cash Transactions
The list of controls is not exhaustive; rather it is designed to provide examples of suitable mechanisms

Training and awareness	Ensure staff are trained in your procedures regarding the use of cash
	Ensure staff know that you have mechanisms for checking compliance with procedures and that there are consequences for non-compliance (ie termination of employment, prosecution)
Procedures	Set clear rules about use of cash, accountability for cash and storage of cash
	Make someone accountable for cash holdings, appoint a custodian for issue, receipt and holding of cash. If possible have two signatories for issuing cash
	Ensure that only the appointed custodian is authorised to access cash stores, receive or issue cash payments (including access to secure storage facilities)
	Set a clear upper limit on the amounts of cash on hand. If it is necessary to increase or exceed the limit, a written request giving reasons must be submitted for prior authorisation from management
	Any advances should be promptly acquitted
	Do not advance further money until previous advances are acquitted
	Ensure appropriate separation of duties in the handling of cash, including by: • ensuring that the person conducting checks on cash holdings is not also appointed as the custodian to store, receive or issue cash payments • ensuring that the person issuing cash (for payments) is not also able to authorise the payment or disbursement
Security	Ensure cash is stored securely – ie lock it in a safe, put strong procedures in place for access, have a camera on the safe
Record keeping	Create a template for cash recipients to acknowledge receipt or use a receipt book and ask the recipient to sign for receipt
	Obtain receipts or acknowledgements for each payment (where possible)
	Keep thorough records of all transactions
	If recipients are illiterate, have community leaders witness receipt of cash or ask for a photo of the recipient with cash in hand
Verification and deterrents	Liaise with the community to validate cost and/or delivery of goods/services for which cash is issued
	Install signage stating what activities are being undertaken and ways of providing feedback
	Conduct checks to ensure correct procedures are being followed. Checks should be regular but random and unannounced. These checks should be signed off by management