Fraud Risk Management Framework

Policy Ownership and Update Details			
DCR Number:	52927	Version Number:	V8
Approved By:	Executive Leadership Team	Policy Owner:	Head of Finance
Last Review Date:	March 2019	Next Review Date:	March 2021

1. Introduction

Scope Global recognises the responsibility to develop, encourage and implement sound financial, legal and ethical decision-making practices to safeguard its assets and those assets of its clients against loss by fraud. The Framework consists of the Fraud Risk Policy, Fraud Mitigation Strategies and Fraud Reporting Procedures and draws together all prevention, detection and response initiatives adopted by Scope Global.

2. Fraud Risk Management Policy

2.1   Policy statement

Fraud events have the potential to cause serious reputational damage and adversely affect morale. Due to the nature of Scope Global's business - operating in many challenging environments and entering into diverse contract arrangements that involve clients, partners and contractors - the risk of fraud and corruption, be it internal or external, is very real. As such Scope Global recognises that whilst it cannot eliminate the risk of fraud, it can minimise the occurrence and impact by:

- The development and implementation of a Fraud Risk Management Policy, Mitigation Strategies and Reporting Procedures;
- Providing a culture that espouses professional and ethical business practices from staff and service providers/contractors;
- Providing periodic fraud awareness training for employees and contractors;
- Ensuring all employees and contractors are cognisant of Scope Global's Fraud Risk Management Framework and Scope Global's Code of Conduct;
- Providing uniform processes and systems that enables employees and contractors to report actual/suspected instances of fraud;
- Ensuring that policies and processes have been developed to provide preventive measures for key business activities, i.e. segregation of duties in regard to authorisation and payment of invoices;
- Ensuring that system protocols and permissions are actively managed;
- Investigating real or suspected instances of fraud by experienced professionals;
- Seeking prosecution of persons and/or organisations for fraud offences; and
- Utilising lawful avenues to recover money or property lost through fraudulent activity.

2.2.   Scope

This Policy applies to all Scope Global employees, contractors and service providers.

2.3 Value for Money principles

Scope Global is committed to applying Value for Money Principles that requires all funding to be spent in an economical, efficient, effective and ethical manner.

2.4 Enterprise risk register

Fraud Management, including internal and external fraud, is considered a strategic risk of Scope Global and as such is actively managed by Executive Management with oversight from the Board. Key controls have been identified to mitigate Scope Global's exposure to fraud risk which are regularly reviewed and monitored in accordance with the Enterprise Risk Management Framework.

2.5   Roles and responsibilities

2.5.1   CEO and Executive Management

The CEO and Executive Management are responsible for fostering and demonstrating the highest standards of ethical behaviour and ensuring staff, contractors and service providers are aware of their legislative and contractual obligations by providing adequate systems, policy and procedures, resources and training.

2.5.2 Fraud Control Officer

The CEO has delegated the responsibility of the Fraud Control Officer to the Head of Finance.
The Fraud Control Officer's role is to co-ordinate Scope Global's approach to fraud prevention and detection and to co-ordinate the response and escalation of any fraud incident that is detected. The Fraud Control Officer reports fraud events and related action plans to the Executive Group.

2.5.3 Senior Managers

Senior Managers are responsible for implementing fraud risk management strategies for their respective divisions.

2.5.4 All Employees and Contractors

All employees and contractors are required to adhere with fraud management policies and procedures and to report any unusual activity to their manager.

2.6 Definition of fraud and corruption

2.6.1 Fraud

Fraud means dishonestly obtaining a benefit, or causing a loss, by deception or other means. Examples of fraud include but are not limited to:

- Theft;
- Accounting fraud;
- Unlawful use of, or obtaining property and equipment such as computers, vehicles, telephones and other property or services;
- Manipulation of Scope Global records;
- Making or using false, forged or falsified documents;
- Providing false or misleading information, or failing to provide information where there is an obligation to do so;
- Obtaining property, a financial advantage or any other benefit by deception, for example through abuse of the payroll system, time recording system or finance system;
- Wrongly using confidential or sensitive information or intellectual property; or
- Corruption in the tender process, including participation in processes involving facilitation payments for contract award in some jurisdictions overseas.

2.6.2 Corruption

Corruption is the misuse of entrusted power for private gain and encompasses a range of activities and behaviours including bribery, collusion and conflict of interest.

Examples of corruption include but are not limited to:

- Facilitation payments (customary payments to secure or speed up government action such as obtaining a visa or permits).
- Cash payments and kickbacks (cash or commission payments made in exchange for services/goods)
- Political contributions (a contribution made to a political party or campaign)
- Acceptance and payment of gifts or excessive entertainment
- Collusion between two parties (i.e. program recipients and staff officials) in order to procure a benefit or gain (such as prospective scholars colluding with staff or panel representatives to guarantee entry into a program).

Conflict of Interest is another form of corruption that all employees and contractors must be alert to, to ensure that they understand the detrimental impact on reputation it can cause, be it real or perceived. The types of conduct considered to be a conflict of interest include any conflict between the public duty and private interests of an employee/contractor, in which the employee/contractor has private interests which

could improperly influence the performance of their official duties and responsibilities. This extends to conduct which others may perceive to be a conflict of interest. A conflict of interest can arise from avoiding personal losses as well as gaining personal advantage, whether financial or otherwise.

Scope Global is potentially at risk to all types of fraud and corruption. In order to minimise these risks, it has in place prevention and detection strategies to ensure these types of behaviours are deterred in all areas of the business.

3. Fraud Mitigation Strategies

Scope Global manages the risk of fraud and corruption throughout its operations. The following measures have been established:

3.1   Pre-employment / Pre-contractual due diligence

Prior to employment/engagement the following checks are undertaken for all employees and contractors in positions of responsibility (which includes program managers and those employees/contractors that are based offshore):

- National Police Check - Scope Global will proceed with caution in regard to any contract with persons who do not have a clear police check (depending on the circumstances).

For all Contractors, the following checks are undertaken:
- Federal Database checks, including:
    - Australian National Security Listed Terrorist Organisations, which contains a list of terrorist organisations that have been formally declared as involved in terrorism;
    - Consolidated List, which contains a list of persons or entities that have been sanctioned under United Nations Security Council and Australian autonomous sanctions.

For all organisations and contractors, the following checks are undertaken:
- The Asian Development Bank's Sanction List
- World Bank Listing of Ineligible Firms and Individuals

Any instance of a positive Federal Database check must be reported to DFAT Sanctions Section – sanctions@dfat.gov.au

3.2   New employees and contractors

For all new employees and contractors, the following criteria/activities apply:
- Employment contracts and Services Agreements – all employment contracts for employees and Services Agreements for contractors include clauses regarding code of conduct, fraud and conflict of interest;
- Training – all new employees undertake fraud training via the E Learning New Employee Induction module and fraud training is conducted periodically for contractors; and
- Policy Acceptance – all new employees are required to read and sign as confirmation of acceptance Scope Global's Code of Conduct Policy and Fraud Risk Management Policy. All contractors confirm their acceptance of these polices by accepting the terms of their Services Agreement.

3.3   Fraud risk assessments

As part of the Enterprise Risk Management Framework, fraud risk across the organisation is reviewed periodically by the Risk Management Committee.

For all new Programs entered into a risk assessment that incorporates both program activities and operational considerations is developed and periodically reviewed for currency.

For all DFAT funded projects, a fraud risk assessment and fraud control strategy is required to be completed within one month of commencement of an arrangement with DFAT.

3.4   Control assessment

Controls mitigating the risk of fraud are periodically audited by the Fraud Control Officer to ensure ongoing effectiveness and adequacy.

3.5   Program specific strategies

Senior Managers/Program Managers are responsible for developing and maintaining appropriate detection strategies to mitigate the risk of fraud within their programs. These include:

- Regular reporting and testing;
- Site visits;
- Retaining evidence of all expenditure;
- Financial reporting, including tracking actual to budget;
- Exception reporting;
- Maintaining and monitoring audit trails; and
- Periodic management reviews initiated by Scope Global's management team.

3.6   Fraud awareness training

All employees and long term contractors receive training in fraud awareness. Responsibility for the delivery of this training rests with the People and Culture team and the relevant Program Manager and Fraud Control Officer.

4.   Reporting a Fraud

4.1   Mandatory reporting

All suspected fraudulent or other improper conduct coming to the attention of any member of staff or contractor (regardless of its financial impact) must be escalated. If the suspected fraudulent activity relates to the person's immediate supervisor or manager, the matter must be reported to the Head of Finance, (in their capacity as the Fraud Control Officer), the CEO, or another member of the Executive Group.

4.2   Minimum requirements

The information reported should include (if available and without conducting any form of investigation):

- Details and dates of the suspected incident;
- Details of the persons involved (including where relevant, details of the employee, contractor, supplier, member of other external party); and
- The value of the alleged misconduct or fraudulent conduct.

4.3   Protocols when reporting a fraud

When reporting cases of suspected fraud, persons should observe the following guidelines:

- Keep the matter confidential. Inform only those people who have a genuine need to know (for example, the line manager, Fraud Control Officer, CEO or a member of the Executive Group). This is to ensure the principles of natural justice are preserved. It is also important to avoid alerting the person alleged to have committed the fraud;
- If there are any evidentiary documents that may assist with the investigation, do not write, mark or change the documents and minimise any handling; and
- Ensure the documentation is retained in a safe and secure manner.

4.4   Protection of person reporting suspected fraud

Scope Global will do everything possible to protect an employee or contractor who reports a suspicion of fraud in good faith from any form of accusation or punishment. Details of the source of any allegation made against an employee, contractor or an external party, or details of the source of any information relative to such an allegation, must not be disclosed to any person external to Scope Global unless:

- As contractually required or legally compelled to do so;
- Required by the police because of the matter being reported to them; or
- The person making the allegation or providing the information has consented to the disclosure of their name.

Any person making allegations or providing information in relation of an alleged fraud or other matter involving improper conduct must be made aware that the information provided will be relied upon and they may be called upon to give evidence about his or her knowledge of the circumstances.

4.5   Fraud recording

The Fraud Control Officer will create a report (refer to Appendix 1 for report template) ensuring that appropriate details are obtained in relation to each incident. The Fraud Control Officer will also be responsible for maintaining a register of all incidents that captures relevant details including actions taken and resolution status.

4.6   Reporting to external parties

Where the Fraud Control Officer becomes aware of a fraud allegation, the Fraud Control Officer will determine, in conjunction with the CEO, what action is required to further investigate the allegation and/or report to the police and client as applicable.

4.7   External investigative resources

Scope Global does not have a designated fraud unit or a qualified fraud investigator. Where appropriate, external expertise may be sought to assist with an investigation. For example, the Fraud Control Officer may require the appointment of a legal advisor, qualified investigator, or computer forensic specialist. The appointment of third party resources must be approved by the CEO and/or the Board.

4.8   Recovery of the proceeds of fraudulent conduct

Scope Global will actively pursue the recovery of any money or property lost through fraud if there is a strong possibility of success. The decision to recover or not must be documented.

4.9   Reporting obligations to clients

Scope Global will comply with the reporting arrangements as specified within the Head Contract of it clients and ensure that prescribed timeframes and templates are complied with at all times.

5.   Post Fraud Review

5.1.1   Lessons Learned

To ensure continual improvement, all internal stakeholders (i.e. HR, Risk, Finance, Program Managers, Legal et al), are required to provide formal feedback documenting lessons learned from the fraud event. Feedback can include providing recommendations regarding preventative measures, remedial measures or the investigation process itself. The Fraud Control Officer will coordinate the responses from all internal stakeholders and provide a summary to all stakeholders and executive. Relevant internal stakeholders will be responsible for implementing agreed recommended measures and report back to the Fraud Control Officer upon completion. All actions will be recorded in CAMMS to track progress.

5.1.2   Internal control

The Fraud Control Officer will re-assess the adequacy of the internal control environment and implement improvements if deficiencies are identified. Any changes to the control environment will be recorded in CAMMS.

Appendix 1: Example of fraud incident report

Report No. xx: \<date\>

Date of report	
Details of person taking this report	
Details of person making report	
Particulars of the suspected fraud including details of persons suspected of involvement (including position and location if internal), dates of offence, method used to perpetrate the fraud	
Estimated value of any loss (could include cash, asset values, transaction value, etc.)	
How was the incident detected?	
Sources of evidence – witnesses, electronic data, documents	
Date / time and how notified to line manager	
Date / time and how notified to the Board	
How did the incident come to the attention of Scope Global?	
Internal control issues contributing to the incident	
Action taken in relation to internal control issues	
Preliminary investigations undertaken and results	
Further investigations proposed	