



ACCESS Phase II Fraud Control Plan

www.access-indo.or.id
ACCESS

DOCUMENT CONTROL**IDSS**

engaging communities and governments

A *Connell Wagner* companyDocument control ID:D:\ACCESS Phase II\8 Forms and Templates\081013-ACCESS
Fraud Plan-NJF.doc

Rev No.	Date	Revision Details	Author	QA	Approve
0	13/10/08	Draft Document	NJF	PGB	PGB

IDSS

Level 12, 60 Albert Road
South Melbourne, VIC, 3205
AUSTRALIA
Tel: 61 3 8683 1457
Fax: 61 3 8683 1444

ACCESS Phase II

Jl. Bet Ngandang 1, No.1 xx
Sanur, 80033
Bali
INDONESIA
Tel: 62 361 288 428
Fax: 62 361 287 509

Table of Contents

1	Introduction	1
2	Fraud.....	2
2.1	Definition of Fraud	2
2.2	ACCESS Phase II Fraud Policy Statement	2
2.2.1	Zero Tolerance Response	2
3	Fraud Risk Assessment.....	3
3.1	Identifying Fraud Risks.....	3
3.2	Analysing Fraud Risks.....	3
4	Fraud Prevention	4
4.1	Fraud Awareness	4
5	Fraud Detection	5
6	Reporting Fraud.....	5
6.1	Process for reporting suspected fraud	5
7	Fraud Investigation.	6
8	Remedies.....	6
	Appendix 1: ACCESS Phase II Fraud Risk Assessment Profile	7
	Appendix 2: ACCESS Phase II Fraud Risk Profile.....	8
	Appendix 3: Fraud Reporting Template	18

Abbreviations and Acronyms

ACCESS	:	Australian Community Development and Civil Society Strengthening Scheme Phase II
AS/NZS	:	Australian Standard/ New Zealand Standard
AusAID	:	Australian Agency for International Development
CPG	:	Commonwealth Procurement Guidelines
FMM	:	Field Management Manual
IDSS	:	IDSS Pty Ltd
IT	:	Information Technology
Korprov	:	(Kordinator Provinsi) Provincial Coordinator
NGO	:	Non-Government Organization
PC	:	Program Coordinator
PD	:	Program Director
PGA	:	Partner Grant Agreement or Project Grant Agreement
PM	:	Program Manager
POH	:	Program Operations Handbook
QA	:	Quality Assurance

Glossary

Allegation	An allegation is a statement or accusation by a person that an offence has, or may have been committed. This does not require evidence of the offence or identification of suspects but there is usually some stated basis for the accusation.
Commonwealth Fraud Control Guidelines	The guidelines outline the Australian government's requirement that Australian Government agencies put in place a comprehensive fraud control program. http://www.ag.gov.au/aghome/commprot/crjd/LECD/fraud.html .
Conflict of interest	Is a situation in which the impartiality of a person in discharging their duties could be called into question because of the potential (perceived or actual) influences of personal considerations whether these are financial or other. The conflict in question is between official duties and obligations, on the one hand, and private interests on the other.
Control	Control is a process effected by IDSS senior management and other employees, designed to provide reasonable assurance that risks are managed to ensure the achievement of IDSS' objectives.
Deterrence	Strategies designed to discourage people from initiating fraudulent activity.
External fraud	Fraud that is committed by someone from outside of the organization (in this case the organization being IDSS or the ACCESS Phase II Program staff), for example a grant recipient or third party provider/supplier.
Fraud against the Commonwealth	Is defined by the Government of Australia as dishonestly obtaining a benefit by deception or other means.
Fraud Risk Assessment	The application of risk management principles and techniques in the assessment of the risk of fraud to an entity.
Internal Fraud	Fraud committed by an employee of IDSS directly against IDSS or the ACCESS Phase II Program.
Investigation	A search or collation of evidence connecting or tending to connect a person (either a natural person or a body corporate) with conduct that infringes the criminal law or the policies and standards set by ACCESS Phase II.
Prevention	Strategies designed to proactively reduce or eliminate fraud.
Whistleblower	A staff member or Program participant who, whether anonymously or not, attempts to make a report in connection with reportable conduct and where that person wishes to avail themselves of protection against reprisal for having made the report.

1 Introduction

Fraud is a generic category of crime which involves an individual or group of individuals dishonestly obtaining some advantage by means of deception. Perpetrators of fraud may seek to gain money, property, time or information. The means used to perpetrate fraud are varied, as are the opportunities that arise that enable fraud to occur.

The ACCESS Phase II Fraud Control Plan reflects AusAID's policy on fraud and has been designed to comply with the Commonwealth's Fraud Control Policy and Guidelines. This Fraud Control Plan contains guidelines and strategies for fraud prevention, detection, investigation and reporting processes and procedures. This plan should be read in conjunction with the ACCESS Phase II Field Management Manual (FMM) and the Program Operations Handbook (POH).

This Fraud Control Plan focuses on control and prevention at a general level. While the extent of fraud in Indonesia is relatively high, the risks and processes for detecting fraud remain relatively constant. ACCESS Phase II management recognizes that some of the behaviours or actions that may be defined as fraud (refer to section 2) are 'accepted' practice in Indonesia. ACCESS Phase II management wants to stress that ACCESS will not tolerate such practice and will deal seriously with any staff, personnel or contractor found guilty of engaging in fraudulent activities.

The ACCESS Phase II Fraud Control Plan will be made available to all Program staff and will be attached to the ACCESS Phase II FMM. The Fraud Control Plan will also be made available on the ACCESS Phase II website for use by Program partners. All Program partners will be made aware of the existence and content of the ACCESS Phase II Fraud Policy.

The ACCESS Phase II Fraud Control Plan is a dynamic document and will be revised periodically.

2 Fraud

2.1 Definition of Fraud

Fraud is not restricted to monetary or material benefits. It also includes intangibles, such as status and information. For the purposes of this Fraud Control Plan fraud is defined as:

“Dishonestly obtaining a benefit by deception or other means”.

The following is a list of behaviours of actions that would be defined as fraud:

- Theft;
- Obtaining benefits or financial advantage by deception;
- Providing false or misleading information, or failing to provide information where there is an obligation to do so;
- Making, or using, or possessing forged or falsified documents including reports, and receipts,
- Falsifying timesheets;
- Causing a loss, or avoiding or creating a liability by deception;
- Charging ACCESS Phase II for non-delivery or incomplete delivery of services,
- Abusing ACCESS Phase II funded facilities;
- Unlawful use of ACCESS assets, property or services;
- Bribery and corruption or abuse of office;
- Evading payments owed to ACCESS Phase II;
- Conspiracy to defraud;
- Or any similar offences to those outlined above.

2.2 ACCESS Phase II Fraud Policy Statement

ACCESS management strongly supports fraud prevention and management and this is reflected in our policy statement:

ACCESS Phase II promotes the principles of good governance and takes a zero tolerance response towards fraud. ACCESS Phase II staff and partners are required to act in a diligent manner to prevent fraud and are obliged to report immediately to ACCESS Phase II management any suspected cases of fraud both within ACCESS Phase II itself and/or with Program partners and sub-contractors. ACCESS Phase II management undertake to handle, investigate and deal with any reported incidents of fraud in a confidential, professional and prompt manner.

2.2.1 Zero Tolerance Response

A zero tolerance response to fraud means that where fraud is shown to have occurred, ACCESS Phase II management’s approach is to take immediate action to ensure that the perpetrator(s) is/are brought to account and appropriate action taken. Appropriate action will be determined based on contractual obligations to AusAID, and the applicable laws and jurisdiction. In all instances of fraud, both internal and external, where AusAID funds or property has been used, AusAID will ultimately determine if the case is to be reported to the police.

3 Fraud Risk Assessment

Fraud risk analysis must consider not only current threats from internal and external sources but also potential and emerging threats.

The management of fraud risk consists of several related steps, beginning with the identification and analysis of the potential risk. It proceeds from risk assessment to threat evaluation, through to the final selection of the appropriate countermeasures. A fraud risk assessment establishes ACCESS Phase II's fraud risk profile and the nature of ACCESS' operating environment so that cost effective practices can be established to contain or minimise each risk.

ACCESS Phase II has prepared a fraud risk assessment based on AS/NZS 4360:2004 and comprises of two tables:

1. The Fraud Risk Assessment Matrix (refer to Appendix 1)
2. The Fraud Risk Profile (Refer to Appendix 2)

The ACCESS Phase II Program Director takes responsibility for the oversight of the management of fraud risk on ACCESS Phase II. The Fraud Risk Assessment Matrix will be reviewed and updated annually or as required.

3.1 Identifying Fraud Risks

In accordance with the requirements of the Commonwealth Fraud Control Guidelines, the following core areas of possible fraud areas have been identified for the ACCESS Phase II Program:

1. Information technology, information security and the internet;
2. Outsourcing functions;
3. Grants;
4. Tendering processes, purchasing and contract management;
5. Travel allowances and other common allowances;
6. Salaries;
7. Property and other physical assets.

In the Fraud Risk Profile (refer to Appendix 1) individual risks have been identified against these core areas.

3.2 Analysing Fraud Risks

For each of the core areas of fraud risk noted above, a profile has been defined using likelihood and consequence criteria (refer to the Fraud Risk Assessment Matrix in Appendix 2).

The determination of whether a particular fraud risk has a high likelihood of occurrence is fairly subjective and based on past experience and future expectations. The assessment is undertaken with reference to the efficacy of the current controls.

Using the consequence criteria in the Fraud Risk Assessment Matrix, the consequence of a risk occurring (with the current controls in place) is noted. Where fraud involves money, its impact may be measured quantitatively. Where fraud does not involve money, the determination of its impact or consequence is again subjective and typically based on past experience. As with the 'likelihood', the assessment is undertaken with reference to the efficacy of the current controls.

Using the Fraud Risk Assessment Matrix ACCESS Phase II management is able to determine the likelihood of the individual risk occurring and how serious the consequences if the risk occurred. The level of each risk is determined by intersecting the *Likelihood* and *Consequence* levels in the Fraud Risk Assessment Matrix (Appendix 1). The Matrix defines the following levels of risk:

E-Extreme Risk – Unacceptable – detailed action plan required
H-High risk – Unacceptable – needs senior management attention
M-Medium Risk – Acceptable – management aware of risk
L-Low Risk – Acceptable – managed by routine procedures

High or Extreme risks must be reported to IDSS and require detailed plans to reduce the risk to Low or Medium.

4 Fraud Prevention

Fraud, like all crime, can be explained by the presence of three factors:

1. Motivation
2. Opportunity
3. The absence of capable guardianship.

Motivation for fraud is wide and varying and may include such factors as greed, social pressures, addictions and poverty. When motivation and opportunity coincide fraud will invariably follow.

The greatest challenge to preventing fraud lies with designing systems which allow ACCESS Phase II staff to continue working effectively while blocking opportunities for fraudulent activity. All ACCESS Phase II management and reporting systems have been developed to ensure transparency and accountability so that any attempted fraud will be detected. The Fraud Risk Profile (Appendix 2) identifies the various risks as well as measures that are in place to prevent their occurrence.

4.1 Fraud Awareness

The first line of defence against fraud, whether internally or externally, is to create awareness of both the act and the consequences of engaging in fraudulent activity. Current measures in place in ACCESS Phase II to raise awareness include:

1. During their induction, all ACCESS Phase II staff members are made aware of their requirement to prevent and detect fraud as part of their contractual obligations.
2. The IDSS Code of Conduct details the conduct expected of all ACCESS Phase II staff.
3. The FMM outlines detailed policies, responsibilities and procedures for anti-corruption and fraud including prevention, detection, reporting and investigation.
4. The POH outlines policies and procedures for fraud and procurement for Program partners, including fraud control measures.
5. The Financial Manual for grantees clearly outlines partner responsibilities in relation to reporting and fraud and is socialized with partners prior to commencing their grant
6. For ACCESS Phase II partners, all Project/Partner Grant Agreements (PGAs) contain the ACCESS Phase II Fraud Policy and steps taken in the event of financial irregularities. This policy is explained to each grant recipient at the time the PGA is signed.

7. ACCESS Phase II also has in place a whistleblower and grievance hotline which is socialized both within the ACCESS Phase II offices, and with Program stakeholders.

5 Fraud Detection

To maximize the likelihood of detecting fraudulent activity, organizational practices should be transparent and auditable. ACCESS Phase II has purposefully designed all processes and procedures to ensure that they contain suitable checks and certifications and are audited at appropriate intervals. Whilst audits are most commonly associated with financial checks, audits will also include review of systems.

With respect to financial audits, IDSS will conduct internal audits as well as annual external audit of the Trust Account. ACCESS Phase II will conduct financial and systems audits of all grant holders at least once through the life of a grant, and more often if poor financial and/or management practices are detected through regular monitoring visits.

The use of internal and external audits does not guarantee the detection of fraud. Undesirable behaviour or activity which escapes the attention of the audits may be discovered by other means, including chance discovery and reporting of peers. The process for disclosure of fraudulent activity is covered in section 6 below.

6 Reporting Fraud

ACCESS Phase II's ability to respond to allegations of fraud is limited to those activities in which it is directly involved, or indirectly through other parties. Nevertheless, ACCESS Phase II is responsible for the integrity of all its business dealings and therefore has an interest in information relevant to this responsibility.

6.1 Process for reporting suspected fraud

Where fraud is detected or where an allegation comes to notice, it is important that the information is recorded and conveyed immediately to the ACCESS Phase II Program Director (PD) and/or Program Coordinator (PC). The PD/PC will in turn notify IDSS and AusAID.

All cases of suspected fraud are to be reported and the outcome or action recorded.

Key considerations in responding to potential fraud are:

1. Initial referral to the PD or PC (day 1).
2. The PD/PC to promptly advise the IDSS Project Manager (PM) of the potential fraud and what action is being taken (day 2).
3. The PD/PC to ensure that a report is quickly prepared to be discussed with the IDSS PM (day 2-3).
4. Depending on the nature of the fraud and whether or not it involved AusAID funds, an agreed course of action will be decided (day 3-4).
5. Official report made to AusAID if the activity involves AusAID funds or property (day 5).

Where the fraud (suspected or otherwise) involves AusAID funds, ACCESS Phase II is contractually required to report this fraud to AusAID within five working days. As a minimum the report of the suspected fraud must include the following:

- the name of the organisation/individual involved
- A description of the incident including a chronology
- The name of the suspected offender
- Details of any witnesses (if any)
- The current status of action taken (if any)

The template for fraud reporting can be found in Appendix 3.

The PD/PC will report any fraud to AusAID involving AusAID funds or property and update AusAID monthly on progress of the investigation using the Financial Irregularities table.

7 Fraud Investigation.

There must be an investigative and reactive response to any suspected fraud on ACCESS Phase II.

Investigation into alleged fraud may be carried out either internally or externally depending on the type and nature of the allegation.

If the fraud involves ACCESS Phase II staff then the PD may make a decision, in consultation with IDSS, to stand down the staff member temporarily while the matter is investigated.

If the fraud involves grant funds, the PGA will be suspended immediately and an audit carried out by ACCESS Phase II financial staff at the earliest convenience.

Following the investigation, the investigation results will be forwarded to AusAID and the final decision on action, including legal action, will be made by AusAID.

8 Remedies

Where fraud is proven to have occurred appropriate action is to be taken. Where appropriate, prosecution of the individual will be considered. Prosecution will be at the discretion of AusAID where the fraudulent activity involved AusAID funds or property.

Regardless of whether prosecution is undertaken, ACCESS Phase II will vigorously pursue the recovery of monies or property lost through fraud.

Where prosecution is not undertaken, IDSS will consider other available remedies. In certain circumstances, the use of administrative remedies may be appropriate. These can include actions to pursue financial or other penalties, demotion and/or dismissal, greater scrutiny and increased controls.

Appendix 1: ACCESS Phase II Fraud Risk Assessment Profile

E – Extreme risk – Unacceptable - detailed action plan required
H - High risk – Unacceptable - needs senior management attention
M – Medium risk – Acceptable - management aware of risk
L – Low risk – Acceptable - manage by routine procedures

High or Extreme risks must be reported to Senior Management and require detailed treatment plans to reduce the risk to **Low or Medium** where possible.

			Consequence					
			Insignificant	Minor	Moderate	Major	Severe	
Likelihood	Expectation:							
	Is expected to occur in most circumstances	5	Almost Certain	M	H	H	E	E
	Will probably occur at some stage	4	Likely	M	M	H	H	E
	Might occur at some time in the future	3	Possible	L	M	M	H	E
	Could occur but doubtful	2	Unlikely	L	M	M	H	H
May occur but only in exceptional circumstances	1	Rare	L	L	M	M	M	

	Consequence				
	Insignificant	Minor	Moderate	Major	Severe
Development Outcomes	Temporary delay Resource (Intensive)	Short period of impact Isolated impact	Forces reconsideration of Program strategies. Impact across a # of Function Areas/elements	Suspension of Program (or elements) Loss of credibility	Termination of Program Complete loss of credibility
Reputation	Internal Review	Internal management review or audit to prevent escalation.	Special audit required by external party. Ability called into question by AusAID	Intense public, political or media scrutiny. Eg: front page headlines. Poor performance noted on AusAID Contractor's Register	Blacklisted by AusAID. Legal action taken by Client.
Program Process & Systems	Minor errors in systems or processes requiring corrective action. Minor delay without impact on overall schedule.	Policy procedural rule occasionally not met or services do not fully meet needs.	Damaged relationship with partners One or more key accountability requirements not met. Inconvenient but not client welfare threatening.	Strategies not consistent with AusAID's requirements. Trends show service is degraded.	Critical system failure, bad policy advice or ongoing non-compliance. Business severely affected.
Financial	1% of Budget or <\$5K	2.5% of Budget or <\$10K	> 5% of Budget or <\$50K	> 10% of Budget or <\$100K	>25% of Budget or >\$100K

Appendix 2: ACCESS Phase II Fraud Risk Profile

Reference	The Risk (What Can Happen)	Source (How Can This Happen)	Impact (From Event Happening)	Current Control Strategies	Current Risk Level			Acceptability (A / U)	Responsibility
					Likelihood	Consequence	Current Risk Level – 10/08		
1.0	Information Technology, Information Security and the Internet								
1.1	Misappropriating information for commercial advantage	Lack of awareness Poor management	Poor reputation Loss of credibility with AusAID and wider development community Blacklisting	QA controls including document review process Code of conduct Policies and procedures in FMM in relation to Intellectual Property rights	2	1	L	A	PD/PC
1.2	Use of unlicensed software	Lack of reputable suppliers in country	Negative audit result Loss of important data	Budgetting for legal software IT policy in FMM Advising staff of need to install legal software Internal audits of software	3	1	L	A	PC/MIS Mgr
1.3	Claiming cost of software license but using pirate	Not tracking license arrangements	Billing AusAID for goods not received	Procurement policies and procedures in FMM	4	1	M	A	PC/ MIS Mgr

Reference	The Risk (What Can Happen)	Source (How Can This Happen)	Impact (From Event Happening)	Current Control Strategies	Current Risk Level			Acceptability (A / U)	Responsibility
					Likelihood	Consequence	Current Risk Level – 10/08		
	copy		IDSS liable to meet costs	IT policy in FMM Advising staff of need to install legal software Internal audit of software licenses					
1.4	Unauthorized use of the internet and downloading unauthorized material	Staff not aware of ACCESS IT policy Lack of oversight	Breach of intellectual property laws Breach of IDSS code of conduct	IT use policy in FMM MIS Manager oversight role of server Project staff oversight role	3	2	M	A	PS/MIS Mgr/ Korprov
2.0	Outsourcing Functions								
2.1	Payment for goods and services not delivered	Lack of transparent process and procedures for procurement	Outputs not achieved IDSS liable to meet costs	Clear procurement procedures with adequate division of responsibilities Internal audit Monthly review of asset	1	3	M	A	PC/ Finance Mgr

Reference	The Risk (What Can Happen)	Source (How Can This Happen)	Impact (From Event Happening)	Current Control Strategies	Current Risk Level			Acceptability (A / U)	Responsibility
					Likelihood	Consequence	Current Risk Level – 10/08		
				registers					
2.2	Sub-contractors falsifying documents	Lack of transparent audit trail for procurement of goods and services Poor management oversight	Outputs not achieved No value for money IDSS liable for costs	Sub-contractors contracts include fraud policy and provision for audits Internal QA of weekly financial reports Internal review of assets register and supplier invoices Transparent procurement policy and procedures in the FMM. Monitoring procedures in FMM	3	3	M	A	PC/ Finance Mgr
2.3	Misrepresentation of service delivered	ACCESS reliance on Service Provider for information Poor management	Outcomes not achieved IDSS liable to meet costs	Outputs clearly defined in contract Appropriate M&E processes in place	2	3	M	A	PC/ Finance Mgr

Reference	The Risk (What Can Happen)	Source (How Can This Happen)	Impact (From Event Happening)	Current Control Strategies	Current Risk Level			Acceptability (A / U)	Responsibility
					Likelihood	Consequence	Current Risk Level – 10/08		
		oversight		Contracts include provision for audits					
2.4	Misrepresentation of self as employee of AusAID/ IDSS/ ACCESS Phase II	Lack of awareness Lack of field oversight	Poor reputation Liable for unauthorized actions	Policy on representation in FMM and as part of staff and sub-contractor contracts. Monitoring by Program staff	2	3	M	A	PD
3.0	Grants								
3.1	Misappropriation of funds	Poor management by CSO Unaware of reporting obligations Culturally acceptable practices defined as fraud by ACCESS Phase II	Outcomes not achieved IDSS liable to meet costs AusAID dissatisfaction	PGAs include audit provisions PGAs include IDSS Fraud Policy Robust eligibility and selection criteria for Program partners All grant recipients made aware of consequences of fraudulent activities	4	2	M	A	PC/ Finance Mgr

Reference	The Risk (What Can Happen)	Source (How Can This Happen)	Impact (From Event Happening)	Current Control Strategies	Current Risk Level			Acceptability (A / U)	Responsibility
					Likelihood	Consequence	Current Risk Level – 10/08		
3.2	Grantees falsifying acquittal of funds	Misuse of responsibility Lack of understanding of financial reporting requirements Lack of transparent audit trail	Outcomes not achieved No value for money Poor reputation in the community IDSS liable to meet costs	Manual for CSO reporting requirements in Indonesian Financial training for all CSO partners Monthly financial acquittals Robust checking process for financial acquittals by ACCESS staff Audit requirements in the PGA Instituted program for audits of all PGAs	4	2	M	A	PC/ Finance Mgr
3.3	Misrepresentation of service delivered	Grant recipient claiming to not have received something when they had Poor monitoring by	Outcomes not achieved IDSS liable to meet costs	Schedules and delivery expectations made clear in the PGA Robust monitoring processes in place by Program staff	3	3		M	Korprov

Reference	The Risk (What Can Happen)	Source (How Can This Happen)	Impact (From Event Happening)	Current Control Strategies	Current Risk Level			Acceptability (A / U)	Responsibility
					Likelihood	Consequence	Current Risk Level – 10/08		
		Program staff Poor monitoring by CSO staff	AusAID dissatisfaction Local government and community dissatisfaction	M&E procedures and framework included in the PGA. Measures to increase transparency between CSO and community they serve in relation to grant management Project audits					
4.0	Tendering Processes, purchases and contract management								
4.1	Accepting a bribe from a tenderer	Lack of oversight Lack of awareness of policy in relation to anti-corruption	Blacklisting by AusAID Loss of reputation among stakeholders	Clear policies and procedures in the FMM and Program operations Handbook in relation to tender processes. ACCESS policy and procedures in relation to anti-corruption in the FMM	1	5	M	A	PD

Reference	The Risk (What Can Happen)	Source (How Can This Happen)	Impact (From Event Happening)	Current Control Strategies	Current Risk Level			Acceptability (A / U)	Responsibility
					Likelihood	Consequence	Current Risk Level – 10/08		
				IDSS Code of conduct					
4.2	Not following Commonwealth Procurement Guidelines	Awarding contracts without following due process Program team members not following procedure	IDSS liable to meet costs Loss of reputation among stakeholders	Tender processes, procedures and requirements clearly defined in the FMM Internal staff training on procurement procedures	2	3	M	A	PC/ Finance Mgr
4.3	Staff receive commissions from service providers	Program staff not following procedures Staff unaware that receipt of commissions are classified as fraud	Loss of reputation Staff termination leading to potential delays in the Program	Clear policy and procedures in FMM on commissions Staff awareness training Transparent procedures implemented	3	2	M	A	PC/ Finance Mgr
5.0	Travel Allowances and other common allowances								
5.1	Claims made for allowances that the claimant is not entitled to	Insufficient review and approval of travel request forms/ acquittal reports	Reduced reimburseable budget Poor morale	Formal approval and review process of travel request forms and advance acquittals Staff awareness of their	3	2	M	A	PC/ Finance Mgr/ Line Mgrs

Reference	The Risk (What Can Happen)	Source (How Can This Happen)	Impact (From Event Happening)	Current Control Strategies	Current Risk Level			Acceptability (A / U)	Responsibility
					Likelihood	Consequence	Current Risk Level – 10/08		
		Falsified timesheets	Reduced credibility of ACCESS Phase II management	rights and obligations					
5.2	Falsified receipts for travel expenses	Lack of formal receipts in the field Lack of staff awareness on reporting requirements	Reduced reimburseable budget Poor morale Reduced credibility of ACCESS Phase II management	Clear and transparent processes for financial acquittal reports Use of ACCESS Official receipts Staff training in financial reporting Adequate financial review of all acquittal forms	3	2	M	A	PC/ Finance Mgr
6.0	Salaries								
6.1	Overpayment	Human error by payroll	Reduced reimburseable budget IDSS liable for costs	Adequate review and approval processes for payroll reports Audit of accounts	2	2	L	A	PC/ Finance Mgr

Reference	The Risk (What Can Happen)	Source (How Can This Happen)	Impact (From Event Happening)	Current Control Strategies	Current Risk Level			Acceptability (A / U)	Responsibility
					Likelihood	Consequence	Current Risk Level – 10/08		
6.2	Claiming for work not done	Lack of management supervision Insufficient review and approval of timesheets/ Expense claims Falsified timesheets	Reduced reimburseable budget IDSS liable to meet costs Poor morale	Formal review and approval process for timesheets Staff awareness training	2	2	L	A	PC/ Finance Mgr
7.0	Property and other physical assets								
7.1	Theft or misappropriation of Program assets	Lack of security Lack of management scrutiny/ oversight Lack of awareness of staff	IDSS liable to meet costs Delays in work progress Reduction in reimbursebles budget	Regular audit of assets register Insurance policies for all assets Use of security guards at night	4	2	M	A	PC/ Korprov
7.2	False claims against IDSS insurance policy	Lack of oversight	Increased premiums Excluded from future coverage	Review and approval of claim forms	2	3	M	A	PC

Reference	The Risk (What Can Happen)	Source (How Can This Happen)	Impact (From Event Happening)	Current Control Strategies	Current Risk Level			Acceptability (A / U)	Responsibility
					Likelihood	Consequence	Current Risk Level – 10/08		
7.3	Inappropriate use of vehicles	Lack of management oversight Poor internal controls Staff unaware of policies on vehicle use	Insurance may not cover in the event of an accident Poor reputation	Policy on vehicle use in FMM PD/PC monitors use of vehicle	2	2	M	A	PD/PC

Appendix 3: Fraud Reporting Template

The following template can be used for reporting instances of suspected fraud to ACCESS Phase II management.

Describe the alleged fraud – what is the fraudulent activity? Give chronology and timeline, if possible	
Who was the person(s) involved in the fraud– detail name, position and contact details, if known	
Who else might be involved in the suspected fraud?	
What is the extent of the fraud? How much in monetary term if known?	
When did this fraud occur?	
Who else knows about this incident?	
What is the relationship of the alleged perpetrator with the ACCESS Phase II Program?	
What other deceit or dishonest conduct has this person been involved in that you know about?	
How much of what you are reporting is established fact?	
Describe any evidence that you have of that could be used to support the allegations?	
Are there any witnesses, or people who could help or advise in this case? Provide names and details if possible	
Are the perpetrators already aware that people know about this fraud?	
Your contact details (confidentiality will be assured)	

Reports can be submitted to the Program Coordinator at ninaf@access-indo.or.id