

Fraud Risk Assessment for Service Providers



NSW Department of
Community Services

**FRAUD RISK ASSESSMENT
FOR SERVICE PROVIDERS**

This document is also downloadable from
DoCS website www.community.nsw.gov.au

NSW Department of Community Services

Head Office
4-6 Cavill Avenue
Ashfield NSW 2131
Phone (02) 9716 2222

September 2005

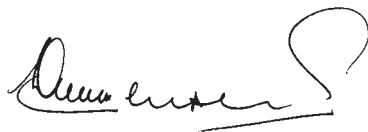
Introduction

This Fraud Risk Assessment has been designed by the New South Wales Department of Community Services (DoCS) to assist you, as one of our service providers, to address the risk of fraud in your organisation. It is based on the same assessment tool that DoCS used recently to determine the fraud exposure within our own Department, but with some necessary amendments.

While I expect that the incidence of fraud is not very high in most of our service providers, fraud can occur when least expected. When it does occur, fraud can be disruptive to the daily activity and morale of the organisation that has been affected, and on occasions can be quite devastating.

On page 2 you will find the segment *How to Use the Fraud Risk Assessment Tool*. This will explain how reading and completing the attached questionnaire will help you. It covers the fraud risks that often occur in a broad range of administrative support functions that most organisations carry out. Broadly, these functions can be summarised under the following categories: Administration; Finance; Human Resource Management; Information Technology; and Procurement.

I thoroughly recommend that you take the time to study and apply this guide.



Neil Shepherd
Director-General

HOW TO USE THE FRAUD RISK ASSESSMENT TOOL

The Assessment is a collection of (1) possible Inherent Fraud Risks that might occur in a series of typical administrative situations, and (2) Recommended Control Measures that could be used to address them.

The Recommended Control Measures are a collection of good ideas that would apply to most situations most of the time. However, there is no “one size fits all” solution. Some Recommended Control Measures may not suit your particular situation, especially if your organisation is rather small.

This is how we suggest you use the Assessment:

- Focus on one Fraud Risk Category at a time (*one category per page eg. Assets on page 4*). Consider all Inherent Risks in the first column. Add any others you can think of.
- Consider each Recommended Control Measure separately. Indicate in the third column *yes* or *no* as to whether or not that control is in place in your organisation.
- Indicate in the fourth column your Risk Assessment Rating, from 1 to 9, where 1 means lowest possible risk and 9 means highest risk. This is your rating of the risk associated with the effectiveness of that particular Control Measure.

RISK ASSESSMENT RATING

Rating	Significance	Definition	Action Required
1	Very Low	Provides no apparent opportunity for fraudulent activity	None
3	Low	Provides a low level of opportunity for fraudulent activity	None-but be aware of any weak spots
5	Moderate	Provides a moderate opportunity for fraudulent activity	Strategy for improvement
7	High	Provides a high opportunity for fraudulent activity	Immediate strategy for improvement
9	Very High	Creates a very high exposure to fraud	Priority strategy for improvement

(Intermediate ratings eg 2, 4, 6 and 8 may be used for gradation).

For example, under Assets, on page 4, the second Recommended Control Measure is *Maintenance of a portable equipment register to keep track of laptops etc.* Suppose you indicated *no* against Control Measure in Place. You would then consider how risky this situation is. If there are no laptops or any equipment of any significant value that staff take away from the office, you might rate the risk as only 1. On the other hand, if there are, and equipment has gone missing in the past, you might rate it 7.

Similarly, on another Recommended Control Measure you may have indicated that the control measure *is* in place. But you still need to determine the level of risk. For example, let us consider the first Recommended Control Measure for Assets *New equipment valued >\$500 immediately given an asset number and placed in assets register etc.* Although an asset register exists, it may not have been updated for some time, so you might rate it 5.

- Add any other useful Control Measures that may occur to you that have not been included in this document, and apply the same rating process.
- Determine and document a strategy to address all Recommended Control Measures that you rated as 5 or more out of 9.
- Total the Risk Assessment Rating column for each page, and determine and enter the Average Fraud Risk (Risk Assessment Rating) for each Fraud Risk Category at the end of each page.
- Transfer the *Sum of risk assessment ratings* for each page to the last page, to determine an Overall Risk Rating for your organisation. This will give you a sense of the vulnerability to fraud of your organisation as a whole.
- But most importantly, **implement your strategies**. If you would like some assistance with this or any other aspect of the Assessment, please don't hesitate to contact your representative from DoCS.

Administration

FRAUD RISK CATEGORY - ASSETS

Inherent Risks - what could go wrong	Recommended Control Measures	Control Measure in Place (yes/no)	Risk Assessment Rating
<ul style="list-style-type: none"> • Loss of assets, particularly “attractive” or portable assets such as laptops or other computer equipment. • Unapproved removal or disposal of assets eg. because of alleged damage. • Loss of control over assets by asset register not being maintained. <p>Additional Inherent Risks:</p>	<ul style="list-style-type: none"> • New equipment valued >\$500 immediately given an asset number/placed in assets register. Assets tagged with the asset number. • Maintenance of a portable equipment register to keep track of laptops etc that are used by individual staff on a temporary basis. • Annual reconciliation of assets on hand (stocktake) to those in the assets register, performed by officer/s independent of receiving or recording function. • Asset disposal to be approved by management, and details documented and retained. • Adequate physical security of assets and premises. • Adequate insurance coverage of assets and premises. <p>Alternative/Additional Control Measures:</p>		
Sum of Risk Assessment Ratings			(a)
Average Fraud Risk			(b)

FRAUD RISK CATEGORY – MOTOR VEHICLES

Inherent Risks - what could go wrong	Recommended Control Measures	Control Measure in Place (yes/no)	Risk Assessment Rating
<ul style="list-style-type: none"> • Unauthorised private use of motor vehicles. • Theft of vehicles from parking areas or while garaged at home. • Theft or exchange of accessories or tools. • Use of petrol card for private vehicle or unauthorised purchases. • Falsification of vehicle log. <p>Additional Inherent Risks:</p>	<ul style="list-style-type: none"> • Policy to convey expectations to staff regarding careful and authorised use of the organisation’s vehicles. • Absences from workplace to be approved by supervisor. • Regular reviews of vehicle log books. • Regular reviews of purchases on petrol cards. • Clearly understood approval mechanism for taking cars. <p>Alternative/Additional Control Measures:</p>		
Sum of Risk Assessment Ratings			(a)
Average Fraud Risk			(b)

FRAUD RISK CATEGORY – GENERAL RESOURCES

Inherent Risks - what could go wrong	Recommended Control Measures	Control Measure in Place (yes/no)	Risk Assessment Rating
<ul style="list-style-type: none"> • Theft or loss of physical resources such as paper, stationery, tools etc. • Unauthorised use of taxi vouchers. • Inappropriate use of telephones (including mobile phones), photocopiers, and portable and attractive items. <p>Additional Inherent Risks:</p>	<ul style="list-style-type: none"> • Organisation's code of conduct distributed to all staff. • Internal policies made available to all staff. • Monitoring of usage/expenditure rates on photocopying, taxis, mobile phones etc. • Retention of invoices for expenditure on above, and system to track expenditure and usage. <p>Alternative/Additional Control Measures:</p>		
Sum of Risk Assessment Ratings			(a)
Average Fraud Risk			(b)

Finance

FRAUD RISK CATEGORY – ACCOUNTS PAYABLE

Inherent Risks - what could go wrong	Recommended Control Measures	Control Measure in Place (yes/no)	Risk Assessment Rating
<ul style="list-style-type: none"> • False invoices accepted resulting in payment for goods not received. • Collusive practice between supplier and purchasing officer resulting in invoice price higher than approved on ordering. • System is manipulated resulting in EFT payments to non-existent supplier. • False staff travel claims submitted. <p>Additional Inherent Risks:</p>	<ul style="list-style-type: none"> • Invoice prices are validated by supporting documentation such as requisitions and purchase orders. • Where possible, segregation of duties between purchasing officer and officer authorising payment. • All staff travel claims approved by the supervisor. • Two signatures on cheques, and signatures registered with the bank. • Blank cheques are not signed. • Payments made on the basis of original invoices, and documentation stamped "paid." • Accounts payable ledger reconciled monthly to the general ledger. • Bank reconciliations performed monthly, and reviewed and signed off by someone independent of the preparer. • Internet payment or funds transfer requires the authorization of two designated individuals. <p>Alternative/Additional Control Measures:</p>		
Sum of Risk Assessment Ratings			(a)
Average Fraud Risk			(b)

FRAUD RISK CATEGORY – ACCOUNTS RECEIVABLE (CLIENTS’ FEES)

Inherent Risks - what could go wrong	Recommended Control Measures	Control Measure in Place (yes/no)	Risk Assessment Rating
<ul style="list-style-type: none"> • Revenue owing by clients for services provided may not be collected by the accounts receivable officer <i>(particularly in regard to relatives or friends)</i>. • Revenue collected from clients for services provided may be misappropriated by collecting officer. <p>Additional Inherent Risks:</p>	<ul style="list-style-type: none"> • Reconciliation of clients’ fees receivable <i>(based on clear records of services provided)</i> to money actually received from clients, by a person independent of the collection process. • Reconciliation of money received from clients to money actually banked, by a person independent of the banking process. <p>Alternative/Additional Control Measures:</p>		
Sum of Risk Assessment Ratings			(a)
Average Fraud Risk			(b)

FRAUD RISK CATEGORY – PETTY CASH AND CASH RECEIPTS

Inherent Risks - what could go wrong	Recommended Control Measures	Control Measure in Place (yes/no)	Risk Assessment Rating
<ul style="list-style-type: none"> • Use of petty cash for private purposes. • Submission of bogus petty cash claims. • Receipts not issued for money received. • Under-banking or failure to bank cash receipts. • Misappropriation of funds. <p>Additional Inherent Risks:</p>	<ul style="list-style-type: none"> • Policy on what can be claimed through petty cash. • Paying officer should stamp claims and receipts as “paid” . • Claims not to be paid without authorisation. • Petty cash claims should contain details of the item purchased. • Adequate physical security over cash holdings eg. access to locked box or safe and combination limited, safe locked etc. • Procedure in place to enable regular reconciliation between documentation, cash receipts and petty cash claims. <p>Alternative/Additional Control Measures:</p>		
Sum of Risk Assessment Ratings			(a)
Average Fraud Risk			(b)

Human Resources Management

FRAUD RISK CATEGORY – PAYROLL

Inherent Risks - what could go wrong	Recommended Control Measures	Control Measure in Place (yes/no)	Risk Assessment Rating
<ul style="list-style-type: none"> • Unauthorised appointments. • Unauthorised overtime worked. • Timesheets altered to increase hours, allowances etc. • Payments above approved entitlements. • Overpayment of employees. • Fraudulent recording of attendance/time. • Leave taken exceeds entitlement. • Inappropriate rosters eg. favouritism, excessive staff. <p>Additional Inherent Risks:</p>	<ul style="list-style-type: none"> • Limited access to payroll. • Supervisors approve staff timesheets or attendance variation forms to payroll. • Appropriate delegations and procedures for appointment of staff. • Monthly management reports (signed off) showing changes to payroll including new hires, resignations, promotions and rates. • Process in place to ensure data entry and data review done by different staff. This applies to both regular payroll and changes such as new employees, pay rates, deductions etc. • Regular management reviews of rosters. • Regular management reviews/reports of major cost fluctuations, eg. overtime worked and annual leave accumulation > set levels. <p>Alternative/Additional Control Measures:</p>		
Sum of Risk Assessment Ratings			(a)
Average Fraud Risk			(b)

FRAUD RISK CATEGORY – PERSONNEL

Inherent Risks - what could go wrong	Recommended Control Measures	Control Measure in Place (yes/no)	Risk Assessment Rating
<ul style="list-style-type: none"> • Applications for employment using false personal details. • Collusion between staff to cover unauthorised absenteeism. • Stealing time eg. conducting personal business during working hours. • Fraud committed through negligence as a result of manager/supervisor not checking claims for payment. • Fraudulent worker's compensation claims. <p>Additional Inherent Risks:</p>	<ul style="list-style-type: none"> • Policies for new staff, terminations and OH&S. • Thorough reference checks carried out on new employees. • Copies of original documentation required to verify personal details including qualifications. • Suspicion of fraudulent worker's compensation claims reported and investigated. • Regular checks of all staff for criminal records. <p>Alternative/Additional Control Measures:</p>		
Sum of Risk Assessment Ratings			(a)
Average Fraud Risk			(b)

Information Technology

FRAUD RISK CATEGORY – INFORMATION TECHNOLOGY

Inherent Risks - what could go wrong	Recommended Control Measures	Control Measure in Place (yes/no)	Risk Assessment Rating
<ul style="list-style-type: none"> • Intruders or inappropriate staff gaining computer access. • Exposure of confidential information. • Tampering with administrative/ financial records. • Excessive internet browsing. • Illegal (pirate) software installed. • Loss of data following accident, resulting in people taking unfair advantage of situation (<i>eg. stealing assets not recorded, demanding inappropriate payments etc</i>). • Inappropriate Internet funds transfer by unscrupulous employee. • Confidential Internet banking details stolen and misused by outsiders. • Corruption of data by hackers. <p>Additional Inherent Risks:</p>	<ul style="list-style-type: none"> • Computer users require unique passwords for access. • No shared passwords. • Passwords regularly re-set. • Restricted access to specific records eg. payroll, general ledger. • Physical security of computers at all times, particularly when office unattended. • Computer users lock work stations when unattended for long periods eg lunchtime. • Staff leaving the organisation have computer access deleted as soon as they have left. • Rules conveyed around the use of the internet, and regular checking of private internet usage, including reviews of monthly internet bills. • Staff reminded not to install illegal (pirate) software. • Rules conveyed around the installation of private software. • Regular backup and proper labelling and off-site storage of important systems and data. • Suspicion of any e-mail from someone unknown or untrustworthy- deletion without opening of any suspicious e-mails, particularly with attachments. 		
Sum of Risk Assessment Ratings			(a)
Average Fraud Risk			(b)

FRAUD RISK CATEGORY – INFORMATION TECHNOLOGY

Inherent Risks - what could go wrong	Recommended Control Measures	Control Measure in Place (yes/no)	Risk Assessment Rating
	<ul style="list-style-type: none"> • Not opening, running, installing or using programs/files obtained from a person or organisation not known to be trustworthy. • Scanning of new programs/files for viruses before opening, running, installing or using them. • Keeping computer up-to-date with anti-virus, firewall software and the latest patches. • Installation of software that will filter spam e-mail or use of an Internet Service provider (ISP) that will filter spam prior to delivery at your inbox. (Spam filters are often included in anti-virus software). <p>For Internet banking:</p> <ul style="list-style-type: none"> • Restriction of Internet banking access to a limited number of authorised individuals, whose passwords are confidential to them and changed periodically, and deletion of access when those people leave the organisation. • Requirement for Internet funds transfer to have the approval of two designated individuals. • Not providing personal details including customer ID or passwords in response to any e-mail. (A bank will never ask you for any private password and this important information should never be shared with anyone). 		
Sum of Risk Assessment Ratings			(a)
Average Fraud Risk			(b)

FRAUD RISK CATEGORY – INFORMATION TECHNOLOGY

Inherent Risks - what could go wrong	Recommended Control Measures	Control Measure in Place (yes/no)	Risk Assessment Rating
	<ul style="list-style-type: none"> • Not clicking on a link or attachment in an e-mail which purportedly sends you to a bank's website. (Access your bank's Internet banking logon page only by typing the address into your browser). • Use of passwords or PINS (Personal Identification Numbers) that are easy to remember but hard to guess. (They should not be relevant to your personal or work situation. Passwords with telephone numbers, postcode, your name, or the name of a close relative or work colleague, and dates of birth are simple for criminals to trace). Creation of passwords with letters and numbers that cannot be easily attributable to you or your organisation. • Memorisation of your password or PIN and not writing it down or storing it on your computer, including in any system or on the programmable function keys. (You are responsible for keeping this information confidential, even from relatives and friends). • Changing passwords regularly and not using the same password for other services such as your video store. 		
Sum of Risk Assessment Ratings			(a)
Average Fraud Risk			(b)

FRAUD RISK CATEGORY – INFORMATION TECHNOLOGY

Inherent Risks - what could go wrong	Recommended Control Measures	Control Measure in Place (yes/no)	Risk Assessment Rating
	<ul style="list-style-type: none"> • Confirming that your data is encrypted between your computer and the bank by looking for the key or padlock symbol on the (usually bottom right hand) corner of the browser window. • Always logging out from the Internet banking menu when you finish all of your banking. • Closing your Internet browser after logging out at the end of each Internet banking session. • Being aware of any windows that 'pop up' during an Internet banking session and being very suspicious if it directs you to another website which then requests your customer identification or password. • Avoiding using shared computers at public places, such as Internet cafes, to conduct your Internet banking. • Looking after your account details if you save or print them after electronically accessing them from the bank's system. Keeping this information in a safe and secure place or destroying it once you have finished with it. • Always checking your statements for any transactions that look suspicious. (If you see any transactions that you did not undertake, immediately report this to your bank). 		
Sum of Risk Assessment Ratings			(a)
Average Fraud Risk			(b)

FRAUD RISK CATEGORY – INFORMATION TECHNOLOGY

Inherent Risks - what could go wrong	Recommended Control Measures	Control Measure in Place (yes/no)	Risk Assessment Rating
	<ul style="list-style-type: none"> Being aware of 'phishing' e-mails that purport to be from a bank or another legitimate business, asking for confidential information. (Most 'phishing' e-mails do not address you by your proper name because they are sent en masse to thousands of recipients. They sometimes contain typing errors and grammatical mistakes, even if they include the banks' registered logos. <p><i>(If you have responded to a 'phishing' e-mail or you have inadvertently entered your personal information on a 'ghost' website, it is always best to seek guidance from your bank. Do not delay in contacting your bank as staff can assist with advice on your next steps. Keep the bank's customer helpline handy in the office. In addition, you should report the crime to your local police.</i></p> <p><i>The bank may need to do an investigation if there is any suspicion that a fraud has been committed. If the investigation proves that you are an innocent victim and have not contributed to the loss, the bank may refund the loss).</i></p> <p>Alternative/Additional Control Measures:</p>		
Sum of Risk Assessment Ratings			(a)
Average Fraud Risk			(b)

Procurement

FRAUD RISK CATEGORY – INVENTORY (STORES)

Inherent Risks - what could go wrong	Recommended Control Measures	Control Measure in Place (yes/no)	Risk Assessment Rating
<ul style="list-style-type: none"> • Theft of goods. • Goods taken for personal use. • Unauthorised disposal of goods. <p>Additional Inherent Risks:</p>	<ul style="list-style-type: none"> • Adequate physical security maintained at the stores. • Regular reviews of the reasonableness of stores requisitions. • Regular stocktakes with results documented and reported to line management. • Persons independent of the stores to be involved in stocktakes where possible. • Line management approval required for disposal. <p>Alternative/Additional Control Measures:</p>		
Sum of Risk Assessment Ratings			(a)
Average Fraud Risk			(b)

FRAUD RISK CATEGORY – PURCHASING

Inherent Risks - what could go wrong	Recommended Control Measures	Control Measure in Place (yes/no)	Risk Assessment Rating
<ul style="list-style-type: none"> • Staff with a personal/pecuniary interest in purchase or contract. • Collusive practices between supplier and purchasing officer. • Purchase of goods for private use. • Officers with delegation for requisition/purchase orders also signing for goods delivery. • Orders fraudulently changed. • Kickbacks or spotting fees paid to staff for preferential selection. • Purchasing through the Internet via a fake website, resulting in theft and misuse of your credit card details. <p>Additional Inherent Risks:</p>	<ul style="list-style-type: none"> • Personal and/or pecuniary interests are declared and registered including any interest in any firm with which your organisation conducts business. • Wherever possible, all purchases to be made through a desirable purchasing individual or section, using purchase requests and orders signed by the appropriate person. • Limited access to purchase requests and orders and (where IT systems exist) to input screens for purchase requests or orders. <p>When purchasing through the Internet:</p> <ul style="list-style-type: none"> • Dealing only with merchants in whom you have a degree of trust - for example, those with a reputable trading name or brand, or with whom you have previously purchased goods in the store or over the telephone. • Looking for the merchant's contact details on their website and calling them to help verify their authenticity. Asking friends and colleagues if they have successfully purchased from the merchant previously. 		
Sum of Risk Assessment Ratings			(a)
Average Fraud Risk			(b)

FRAUD RISK CATEGORY – PURCHASING

Inherent Risks - what could go wrong	Recommended Control Measures	Control Measure in Place (yes/no)	Risk Assessment Rating
	<ul style="list-style-type: none"> • Looking for the key or padlock symbol on the merchant's web browser. (This will indicate whether or not the merchant's site offers an encrypted line of communication to protect your details). • Not sending your credit card details via insecure means such as e-mail that is not encrypted. <p>Alternative/Additional Control Measures:</p>		
Sum of Risk Assessment Ratings			(a)
Average Fraud Risk			(b)

Overall Fraud Risk Assessment Rating

For:

Fraud Risk Category	(1) No. of Control Measures rated in each Category	(2) Transfer (a) from each Fraud Risk Category
Administration Assets Motor Vehicles General Resources		
Finance Accounts Payable Accounts Receivable (Clients' Fees) Petty Cash and Cash Receipts		
Human Resource Management Payroll Personnel		
Information Technology		
Procurement Inventory (Stores) Purchasing		
TOTAL		
OVERALL FRAUD RISK EXPOSURE	Divide total of (2) by total of (1)	