Community Underwriting

Insurance by the sector for the sector

MANAGING FRAUD RISK

A Resource to Help Not for Profits Manage the Risk of Fraud in their Organisation

Most Not for Profits operate in an environment of trust due to their charitable objectives, social compassion and generosity.

With limited funds, the core focus is understandably around delivering on the services that drive the organisation and activities that raise additional funds to create goodwill and support the charitable purpose.

Board members however have an important responsibility to ensure that resources are protected so that the organisations' objectives are achieved.

Unfortunately the potential for fraud in a Not for Profit is a key risk exposure and in many instances, is actually higher than in for profit enterprises. The reasons for this are numerous and need to be carefully considered by organisations both big and small:

- Many Not for Profits face significant hurdles providing adequate Board oversight. Most rely on volunteer Board members who lack sufficient experience or training;
- Turnover on Boards tends to be high or conversely extremely long tenures tend to allow a culture of acceptance of the status quo and minimal review;
- Limited resources - by necessity a significant amount of trust is placed in individuals, there is insufficient opportunity for oversight and limited opportunity for independent checks;
- Lower remuneration, limited career advancement and economic circumstances can create financial pressures on individuals which may be further exacerbated through drugs, gambling or spending habits;
- Many organisations rely on reputation and goodwill for survival. A public incidence of fraud can be devastating on the organisations' standing with donors, volunteers, clients and government.

Common forms of fraud include:

- Billing false or inflated invoices;
- Payroll fraud;
- Falsified expense reimbursement;
- Stolen or altered cheques;
- Undocumented / reconciled refunds;
- Unauthorised payments / transfers;
- Theft of property;
- Fraudulent financial reporting;
- Use of organisational resources for personal benefit.

Fraud can occur over an extended period of time and be difficult to detect. Even if your organisation considers the risk of fraud low, controls still need to be put in place and regularly reviewed.

The opportunity for fraud is greater where there is a lack of internal controls, lack of inappropriate management oversight and/or the ability to override existing controls. Your organisation's exposure to fraud can be mitigated through strong Board governance, appropriate internal controls and regular review.

Effective controls are often simple, common sense approaches and do not require elaborate systems or processes to implement.

A review of internal controls needs to consider:

- Are the controls working / have any weaknesses been detected?
- Are there changes in the types of risks since the controls were established (new vendors / payment methods, internal systems, additional sources of funding)?
- Does each procedure still make sense / fit the purpose?
- Are procedures too complex or onerous?
- Are modifications required?
- Are all employees adequately trained on internal controls and what to do if abuse is identified?

Strategies to successfully manage fraud should be considered in three parts:

Prevention - proactive measures to help reduce the risk of fraud occurring.

Detection - controls which should uncover incidents of fraud when they occur.

Response - measures which will allow corrective action to be taken and minimise the impact to your organisation.

There is no absolute approach or mechanism that will prevent all fraud, but by analysing the potential for risk and implementing risk control and risk mitigation strategies you can limit the impact to your organisation and its stakeholders.

The following provides a guide to some of the controls and risk mitigation areas that might be considered. It is by no means exhaustive, but serves as a starting point for organisations to consider the specific risk exposures relevant to them:

Consider	Key Exposure Areas	Example Controls / Risk Mitigation
Accounts Fraud	Unauthorised EFT or cheque transfer to an employee or third party account Credit card abuse Unbanked cash collections False or inflated client transactions Manipulation of accounting systems	• Formal procedures and electronic systems to ensure all revenue and expense transactions across the organisation are captured, validated and provide a detailed audit trail • Preparation of an annual P & L with monthly reporting of variances in income and expenditure • Segregation of duties (e.g. no single person should be responsible for billing, recording funds and/or reconciliation. Where the organisation is small, consider a director or volunteer for the role) • Dual signatories / electronic approval over nominated thresholds • Formal delegations of authority and specific authorisation controls / expenditure limits • No pre-signing of cheques or cheques made to cash / minimal petty cash • Regular bank reconciliations and review of payments by an independent person / external bookkeeper • Enforcement of annual leave / job rotation
Theft / Procurement Fraud	Theft of cash, plant & equipment, stock, donated funds or merchandise Payments to fictitious vendors Altered or fraudulent billing Unapproved removal / disposal of assets Inappropriately awarded contracts Concealed incentives / kickbacks from suppliers	• Procurement processes which address the requisition, authorisation, verification, recording and monitoring of all expenses • All major contracts above determined limit to obtain Board approval • Implementation and maintenance of a formal asset register • Regular documented stock reconciliation • Procedures for the tendering, assessment and awarding of significant contracts • Surveillance security in areas of high value assets • Gifts and benefits policy and register

Consider	Key Exposure Areas	Example Controls / Risk Mitigation
Personnel	Favouritism in the recruitment process Ghost employees Unauthorised incentives / salary increases / manipulation of KPI's Understatement of leave taken Overstatement of hours worked Overstatement of expenses Personal use of the organisations assets or resources	• Background checks on employees and key volunteers (verification of identity, formal qualifications, criminal record and bankruptcy checks) • Formal recruitment process that requires more than one person in the decision making • Limited access to payroll • Audit logs on payroll transactions

Management Accounts	False revenue recognition
	Expense understatement
	Asset overstatement
	Understatement of liabilities
		• Processes for accurate, detailed and informative reporting from management which provide analysis of:
		  • Material earnings and expense variances and updated results forecasting
		  • Liquidity / cash balances
		  • Debtor position
		  • Creditor position
		  • Inventory analysis
		• Transparency of material transactions
		• Internal audit

Commercial Information / Intellectual Property	Theft of client information Business practices and unique procedures	• Physical controls for access, inputing and changing client and other business information • Remote back-up of data to independent location
Conflicts of Interest	Transactions and relationships that can create a perceived or actual conflict of interest	• Personal and pecuniary interest declarations • Board identification and assessment of related party relationships and transactions
Reputational Risk	Negative impact / loss of support from donors, volunteers, clients and/or government	• Formal processes for media management • Formal processes for stakeholder management • Internal announcements
Culture	Lack of accountability Lack of transparency Acceptance of lax controls / inappropriate use of resources Inadequate reporting regime / fear of reprisal	• Board / Audit Committee oversight • Zero tolerance for fraud • Appropriate whistleblower mechanisms • Clearly articulated policies and procedures / code of conduct • Communication and training • Auditing and monitoring / internal control review • Disciplinary action and recovery