Protecting Your Organisation Against Fraud

Everyone is aware of stories of fraud. They often appear in the media and are followed with avid curiosity. People seem to need to understand why fraud happens and why someone imagined they would get away with it.

Perpetrators of fraud are often ordinary, well-like individuals that others trust and respect. Their reasons vary but may relate to financial pressures due to changed circumstances (partner's job loss, etc), gambling debts or living beyond their means, claiming, when caught, that it was only a loan which they intended to repay. Others start and end with criminal intent, an act of revenge or greed.

All organisations are potentially at risk of fraud, including the not-for profit (NFP) sector and it can do considerable damage to the sector. Even a small fraud can have substantial consequences far exceeding the significance or value of the act.

Fraud is generally seen as a financial risk however it can also refer to falsifying documentation (including resumes, insurance claims, research outcomes, etc), conflict of interest and identity theft. Whatever its form, it can severely damage an organisation's reputation and image which in turn can impact on its ability to attract staff, volunteers and funding. It can attract the attention of compliance bodies and may result in additional reporting. Ultimately it can affect an organisation's capacity to operate.

In general, the greater the revenue stream and number of paid employees, the higher the risk of fraud. However this does not mean that fraud does not happen in small organisations dependent on volunteers. All organisations need to prepare against fraud.

Whilst fraud is a risk organisations cannot totally remove, it is possible to put in place strategies and procedures which lessen the likelihood of it occurring and if it does occur, reduce its impact.

What is Fraud?

There is no set definition of fraud. Definitions tend to cover a similar area but each is slightly different. It has been defined as *"an act of deception intended for personal gain or to cause a loss to another person or organisation."*[1] It has also been described as "the *use of dishonest or deceitful conduct in order to obtain some unjust advantage over someone else*."[2] Other definitions refer to it being an intentional act and others note it may be a wrongful act but not necessarily criminal.

Fraudulent activities in the NFP sector can include appropriation of assets (financial, fixed and intellectual property), false accounting (financial statements, contracts and acquittals) falsifying of documents (qualifications, experience and identification) and corruption (bribery, kickbacks and conflict of interest).

[1] Australian Crime Commission *Nature of Frauds*

[2] Lozusic, Roza (2003) *Fraud and identity theft* NSW Parliamentary Library Research Service, [Sydney] p 2-3

In recent years there has been a rise in online fraud, involving both financial (eg payroll and credit card transactions) and non-financial (eg confidential client records) data.

As noted above the impact on the organisation can go far beyond the initial act, particularly if it gets out into the public arena. It can damage confidence and staff morale, erode trust and disempowered the organisation.

Cost of fraud can include:

- financial losses
- reputation and brand damage
- increased regulatory and audit overheads
- exposure to legal risks resulting from violating privacy
- loss of business/partnership opportunities as a result of lack of trust
- impact of computer downtime resulting from attacks
- increased insurance costs
- potential penalties
- difficulties in attracting/retaining staff and volunteers
- reduction in service capacity.

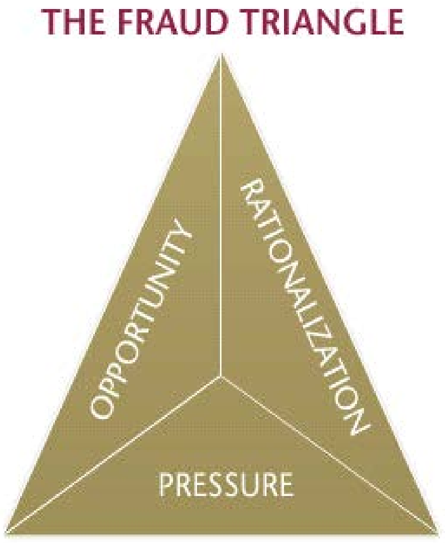
Factors influencing fraud

Fraud is about opportunity. It can be the result of:

- misplaced trust
- inadequate hiring and supervision processes
- weak or non-existent internal controls
- inadequate security
- lack of accountability
- overly broad access to information, particularly online information
- poor ethical culture.

Opportunity however is only one part of the equation. Donald Cressey[3], an American criminologist, concluded that three factors were likely to be present in any fraud event. He referred to this as the Fraud Triangle:

[3] McNeil, Andy The role of the board in fraud risk management in *The Conference Board*



- *Pressure* or motivation refers to the event(s) or situation(s) that lead the individual to consider the possibilities. This may include gambling or financial problems, maintaining a desired lifestyle or revenge against the organisation.
- *Rationalisation* is the reason used to justify the act ie *"It's only a loan, I was going to repay it"; "I'm only taking what I should have been paid."; "Because I can!"*
- *Opportunity* is the weakness in the system that allows the fraud to occur if there are no measures in place to limit the opportunity, temptation is easily created, exposing the organisation to a greater chance of fraud.

It is unknown whether the opportunity to enact fraud precedes or follows the pressure to consider the possibilities.

Avoiding Fraud

Even if an organisation rates its fraud risk as low or not an issue, strategies protecting against fraud still need to be put in place and regularly monitored.

There are two significant factors identified with decreasing the likelihood of fraud:

- A strong ethical culture with a clear commitment to integrity and ethical values clearly modelled by the board and management
- Management approaches that ensure strategies are in place to protect the organisation from fraud rather than just accepting it as an inherent risk.

Ideally this would occur within a positive working environment which encourages employees to follow established policies and procedures and act in the best interest of the organisation. There would also be a clear organisational structure with open lines of communication, clarity of responsibilities and positive employee and volunteer recognition.

Implement physical access controls also assist in avoiding fraud. Access to premises, computer systems, client files, etc should only be provided to those who need it to perform their job. This would also include regularly changing computer and building access codes.

Best practice suggests there are three steps to mitigate against the risk of fraud:

- Prevention – controls designed to reduce the risk
- Detection – controls designed to uncover risk when it occurs
- Response – controls designed to facilitate corrective action and harm minimisation.

In addition to specific fraud policies, procedures, etc aspects of these should also be incorporated into other relevant policies (eg Governance, Financial, HR, IT, etc)

Prevention controls

- Fraud Risk Assessment
- Fraud Control Strategy including a fraud and corruption policy, fraud risk plan and fraud risk register Code of ethics/conduct
- Conflict of interest policy / Declaration / Register (See Policies
- Strong internal controls (eg Policies and procedures, segregation of duties, enforcing annual leave, etc) Staff screening when employing, promoting or transferring to high risk areas, specifically in relation to checking qualifications and experience.
- Effective and consistent supervisory processes – this is particularly important for small NFPs that have difficulties segregating duties or where employees are working in isolation.
- Due diligence checks on suppliers and contractors
- Training for staff and volunteers to increase awareness of ethics and risk management processes and strategies
- Employee support programs
- Independent audits. Many organisations place considerable emphasis on having "trustworthy" staff and/or volunteers as a protection against fraud. Taking into account the number of "trustworthy" staff implicated in fraud cases[4]this is probably not a foolproof strategy.

Detection controls

- Continuous internal monitoring and auditing of procedures and processes.
- Allocation of resources for fraud detection
- Proactive data analysis. Fraud detection software is available to monitor and analyse data collected in the normal course of business.
- Mechanisms to report fraud which protect the individual (ie whistleblowers) providing the information
- Conduct unannounced financial and asset audits
- Fraud stress testing (ie a controlled attempt to perpetrate fraud to test the effectiveness of fraud controls particularly where manual controls are key to prevention and detection).

Response Controls

All organisations should have an internal investigation unit or working party in place and a fraud response plan which would include

- Who manages an allegation of fraud
- Who should conduct an investigation

[4] Laslett, Glen & Steinberg, Gavin Preventing fraud

- Who can conduct an investigation
- Who should be told, when and what
- What insurance cover against fraud is held and the notification period required
- The legal obligation of an individual once fraud has been detected
- How to deal with the perpetrator
- How to deal with media and stakeholders
- Whether the organisation has decided it is mandatory to report fraud to the police.

Under NSW and Commonwealth legislation, not all fraud is considered a criminal act. Where it is considered criminal there is a duty to report it to the police in NSW under section 316 of the Crimes Act 1900 (NSW)

Any investigation needs to be completed by someone with the necessary skills as the process must be seen to be lawful and admissible, as well as having natural justice and procedural fairness where the evidence is preserved (ie will stand up in court). It is probably advisable to employ an external investigator or contact the police.

Other policies and processes that could be considered include:

- Disciplinary policy
- Police referral policy
- Review of all relevant internal controls and policies subsequent to identifying a fraud.

Role of the Board and Management

The Board is responsible for managing the organisation and protecting its assets. As such they are responsible for ensuring that some or all of the above strategies are in place to protect the organisation from fraud. Generally these activities are delegated to Audit/Finance Committees, Risk and Compliance Committees and/or senior staff. Irrespective they need to provide a regular overview of relevant information and an opportunity to ask questions providing further detail.

It is the Board’s responsibility to instil an ethical organisational culture which operates with integrity. Specifically they need to:

- Ensure appropriate policies and internal controls are implemented and regularly monitored
- Review compliance with contractual agreements, regulations and legislation
- Understand the fraud-related programs and controls and independently assess and monitor their effectiveness
- Ask penetrating and difficult questions of management
- Evaluate whether oversight mechanisms are in place and functioning to prevent, deter or detect overriding of internal controls
- Show clear commitment that is supported where necessary with resources.

Management's role is to ensure accountability is in place and adhered to and that all staff understand the importance of internal controls and appreciate why things must done in a certain way.

Both the Board and management must lead by example and set the tone as they set the benchmark for the required behaviour.

References and Resources

In addition to the material below, there is a considerable amount of information available on the internet that is easily accessed by a search engine. This includes documents prepared by NSW government agencies and NFP organisations eg policies, charters, checklists, frameworks and plans.

BDO Australia

- Not-For-Profit Fraud Survey
  PDFs of the 2014 and 2016 surveys are available to download.

NSW Family and Community Services (FACS)

- Fraud Prevention Chapter 7 in Good Governance: It's your business
  Includes industry case study training resources, also has a Fraud and corruption control policy and plan. Much of the information and checklists are aimed at large organisations.

NCOSS Sector Support

- Templates and Resources
  - Board Delegations
  - Ethical frameworks: Codes of ethics and conduct
  - Managing Conflict of Interest
  - Probity and Governance

Whistleblowers

- How to encourage whistleblowers (Risk Management Magazine – Griffith University)
- SAMPLE Employee Protection (Nonprofit Risk Management Center)
  Example of a Whistleblower Policy

Online data security

- Data Security for the Not-for-Profit Sector
  Overview of what needs to be considered when developing policies and procedures to protect all forms of sensitive data.

- PCI Compliance for the Not-for-Profit Sector
  Online security for credit card payments – Outlines the requirements of PCI compliance, how to assess products, outsourcing credit card management services.

Risk Assessment Tools

- Guide to Fraud Risk Assessment (NSW Department of Community Services)
  The Guide describes a range of possible inherent fraud risks that might occur in a series of typical administrative situations and control measures that could be used to address them

- Fraud Risk Assessment for Service Providers (NSW Department of Community Services)

Tool for assessing risk in a service organisation

Fraud Policies

- Fraud Control Policy and Management Plan (Jobs Australia)
  The template incorporates a fraud policy, control plan, risk register and a whistleblower policy

Guide on internal controls

- Internal controls for not-for-profit organisations (CPA Australia)
  The checklists contains refers to all types of fraud risks, not just financial. Outlines of general strategies to manage risk, risk assessment questions, examples of internal controls and checklists specific to payroll, cash receipts/payments, etc. are also included here.

NB: The above websites were accessible on 8 Dec 2015. If the links do not work search on the title of the document or go directly to the website of the organisation.