The Institute of Internal Auditors Australia

White Paper –
Fraud Risk Indicators

January 2017

© The Institute of Internal Auditors–Australia
Level 7, 133 Castlereagh Street
Sydney NSW Australia 2000
Telephone: 02 9267 9155
International: +61 2 9267 9155
E-mail: enquiry@iia.org.au

Table of Contents

Table of Contents 3
1. Background 4
  1.1 Purpose 4
  1.2 Background 4
2. Discussion 5
  2.1 Issue 5
  2.2 History 5
  2.3 Discussion 5
3. Conclusion 9
  3.1 Summary 9
  3.2 Conclusion 9
4. Bibliography and References 10
  Bibliography 10
  References 10
  Purpose of White Papers 10
5. Author's Biography 10
6. About the Institute of Internal Auditors–Australia 11
7. Copyright 11
8. Disclaimer 11

1. Background

1.1 Purpose

When designing, assessing or monitoring internal controls, undertaking probity activities, or conducting internal audits, it is considered appropriate to take cognisance of the indicators of fraud.

1.2 Background

Fraud can be a substantial threat to an organisation. It has been stated that all organisations are subject to fraud risks[1] and it has been reported that fraud is five percent of an organisation's annual revenues.

Fraud is a threat to revenue, assets, brand, reputation and other resources and may result in significant penalties, political consequences, operational and strategic limitations and may even be an existential threat to the organisation.

Where those working with internal controls or audits do not use fraud indicators it is likely that many frauds will remain undetected, resulting in potentially significant cost to the organisation.

Where people use fraud indicators without understanding them they run the risk of failing to detect a significant number of frauds.

The value of fraud indicators has often been limited by people using pre-prepared lists of indicators that do not take into account the specific environment within which the auditee operates or the staffing of the area.

Using fraud indicators and a structure such as is contained in this white paper to apply the indicators to specific situations is likely to substantially increase an organisation's ability to mitigate the risks of fraud.

Fraud is defined in the glossary to the *International Standards for the Professional Practice of Internal Auditing* (IIA Standards) as "any illegal act characterised by deceit, concealment, or violation of trust" and in the COSO *Fraud Risk Management Guide* as "any intentional act or omission designed to deceive others, resulting in the victim suffering a loss and/or the perpetrator achieving a gain".

---

[1] *Fraud Risk Management Guide* viii

2. Discussion

2.1 Issue

Fraud indicators are a useful and effective tool in mitigating the risks of fraud.

2.2 History

Using indicators is useful for compliance with IIA Standards, especially 1210.A2, 2010, 2120.A2 and 2210.A2. It is also useful for principle 8 of the COSO *Internal Control – Integrated Framework*. Indicators have long been used in audits, probity activities and internal control management. Fraud indicators have proven especially useful in many environments, yet they typically remain under-utilised and are sometimes applied in a rote manner. It is hoped this white paper will help to advance the field.

2.3 Discussion

In order to help ensure that all useful indicators are taken into account it is helpful to consider two categories, the first is the footprint that is left behind by a fraud act, and the second is the fraud triangle.

The fraud triangle indicates that fraud requires three components: perceived pressure, perceived opportunity and rationalisation. Pressure refers to the pressures on a person to perpetrate a fraud, opportunity is the means by which the fraud is committed and rationalisation is the cognitive state that allows the perpetrator to justify the fraud. Each of the components has indicators.

Footprints of fraud

When developing corruption indicators, it is helpful to consider the evidence left behind by a fraudulent act. You may think of indicators as analogous to the indentation in mud that is left by feet bearing a person's weight. Leaving a trail is not intentional, but is often unavoidable. The footprints of fraud may refer to the transaction, the perpetrator or the method of hiding the fraud.

The process for developing these indicators is to consider how the frauds would be perpetrated and what signs they would leave behind. Examples are:

- The transactions or activities are undertaken at an unusual time.
- The names used in the transactions indicate that the perpetrator was showing off[2].
- There are unusual, excessive or suspicious overrides, duplications or cancellations of transactions.
- Transactions are split to avoid notice/delegations or transactions with missing requirements.
- Documentation is incomplete, difficult to find, has missing elements, or has evidence of changes, deletions or additions.
- Only one person processes particular transactions, including only one person transacting with a particular supplier or handling certain decisions/negotiations where this is unusual.

---

[2] Examples are M. Yass in which one needs to move the dot one letter to the right to understand, Alfred Capone which is Al Capone, the names of the Cambridge spies working for the Soviet Union and a dummy company set up which was a word made up of the first four letters of the initial of each of the perpetrators.

- Particular transactions are unusual because of the number, value or type of those transactions or because they differ from expectations, industry experience and the region's or organisation's history.
- The transactions are the result of *tidying up* reconciling or suspense items, or are unusual transfers between accounts.
- The transactions result in key performance indicators being met.
- The transactions do not make sense individually or cumulatively, or the mix of transactions appears wrong.
- Transactions are processes by people who would not normally process those transactions.

It is useful to consider how you would hide a fraud in order to identify relevant indicators. Examples include getting someone else to process or authorise the transaction or verify proof of delivery, using someone else's password, disclosing one's password to others, processing transactions when others are not around, changing characteristics of transaction, not involving others who should be involved, leaving out parts of the transaction or process, getting someone to legitimise/offset the fraud, and manipulating the transaction so that it will not attract scrutiny[3].

Pressure

Pressures on a person to perpetrate fraud may include financial pressures, including due to the economy, addictions, health problems, family circumstances and a desire to live well beyond one's means; threats to safety from criminals or others who have something to gain or potentially lose; social pressures from colleagues; career pressures from managers and supervisors; social pressures from those to whom one has a loyalty, including romantic interests, relatives, people from one's neighbourhood or one's religious or social network; and psychological pressures, including a pathological need to impress others, depression and mental illness.

Any indicators of these pressures should be considered including a financial problem that seems to suddenly disappear, a lavish lifestyle, consorting with criminal elements or associates, colleagues or managers are suspected of engaging in fraud, seemingly favouring individuals to whom one is socially connected, falsely claiming significant qualifications and/or experience, and evidence of poor ethical decision-making.

The pressure may arise from the organisation's failure to implement measures to improve the ethical relationship between its employees and the third parties they interact with. Examples are that third parties may offer excessive gifts and benefits, create conflict of interest situations through promises of employment, groom employees, offer bribes, and encourage their staff to seek employment in your organisation. Failing to have, communicate and enforce appropriate codes, policies and standards may thus be indicators of fraud.

Rationalisation

In order to work out the rationalisation indicators of fraud, it is useful to consider what the attitude is of perpetrators that allows them to justify to themselves committing a fraud. People may be able to justify perpetrating fraud when the organisation has not adequately clarified the difference between acceptable and unacceptable conduct, or is lax in following or enforcing it. Individuals may justify perpetrating fraud when they have a sufficiently negative perception of management, their colleagues, the organisation or the environment. Psychological issues may also lead to fraud rationalisation.

---

[3] A public sector example is managers of contracts or projects having them finish exactly on budget to avoid scrutiny, where ironically it is unusual for contracts or projects to finish exactly on budget.

Indicators include:

- Inadequate policies or procedures to make it clear where the organisation's ethical line is drawn.
- Training in ethical issues is inadequate, or only gives the organisations stance and does not contain a component to motivate employees to do the right thing.
- A poor ethical culture or subculture, or a perception that managers or supervisors are ethically challenged.
- Poor practices are tolerated such as bullying, harassment, lapses in safety practices, or dishonest treatment of customers or suppliers.
- The person or colleagues have significantly negative attitudes about the ethics of the employer, management, customers, suppliers or the industry.
- A significantly adversarial relationship exists between managers and employees.
- The person perceives that management have failed to provide support when it was needed.
- There is a substantial sense of entitlement.

Opportunity

Usually opportunity arises due to inadequate internal controls or breakdowns in the system of internal control. It may therefore be useful to consider opportunity in terms of an internal control framework. Here the five components from the COSO framework have been used in a broad manner. The components are control environment, risk assessment, control activities, information and communication, and monitoring.

Control environment

Under this component, it is useful to consider the indicators of fraud arising from issues relating to ethical culture, people and structures. Indicators include:

- Staff are not engaged or are actively disengaged as shown by staff surveys, high staff turnover, high absenteeism, poor productivity, high levels of customer complaints or high levels of staff grievances, or complaints against others.
- Limited or poor supervision and management so that people may not carry out control checks properly.
- Employees performing internal controls do not consider certain kinds of fraud to be wrong.
- Some employees are over-trusted.
- Managers do not want to hear bad news.
- The culture is not to question people or certain people.
- The area is perceived as being geographically or structurally removed, or is remote from management.
- Management do not understand area/operations/reports/etc.
- People carrying out controls do not adequately understand what they are doing.

Risk assessment

It is appropriate to consider, from a fraud perspective, if people understand the objectives and risks, including when there are substantial changes. Indicators include fraud control objectives not being properly formulated, communicated or appreciated; certain sources and categories of fraud being ignored for political or other reasons; individual fraud risks not being identified or being underestimated; inappropriate responsibility for fraud identification, and measurement and significant change in the organisation's environment, structure or systems.

Control activities

Indicators include instances where the internal controls to mitigate fraud risks are poorly designed or do not operate properly. Indicators include:

- There is a poor understanding of internal controls, the reasons for performing the controls, and the link between controls, objectives and fraud risks.
- There are internal control problems such as inadequate segregation of duties, poor access controls, ICT control weaknesses, insufficient verification controls, poor supervision, inadequate reconciliations, and deficient controls over standing data.
- Documentation of processes, decision-factors and other key elements is poor.

Information and communication

Indicators are where there is poor communication and use of information to support internal controls to deter fraud, and there is poor communication with external parties. These indicators include where managers and staff with key roles in preventing and detecting fraud do not receive training or adequate information to allow them to meet the expectations placed on them.

Monitoring

Fraud indicators related to monitoring include:

- Limited or no transaction reviews.
- Inadequate management reporting, including key aspects not included in reports, and reports not suitable for finding fraud.
- There is an ability to suppress reports or transactions.
- Results appear questionable, including results that are too good, results not moving for changes in environment, changes out of line with the results of others, and an unexpectedly low number of incident reports.
- Transactions created after initial reports have been produced which significantly improve the position or may disguise profits or sales for future use.

3. Conclusion

3.1 Summary

Incorporating indicators of fraud into internal controls and audits helps ensure the organisation’s resources, reputation and integrity are protected, key stakeholders are satisfied, and strategic and operational objectives achieved. It is important to ensure the indicators used are relevant for the particular circumstances.

3.2 Conclusion

When designing, assessing or monitoring systems of internal control to limit the risks of fraud, it is considered that significant value can be derived from incorporating indicators of fraud into systems of control.

When conducting internal audits, probity reviews and investigations, taking cognisance of the indicators of fraud can substantially reduce the audit risk and increase the likelihood of detecting fraud that could be significant for the organisation, its operations or strategies.

4. Bibliography and References

Bibliography

International Standards for the Professional Practice of Internal Auditing (Standards), Institute of Internal Audits revised October 2016.

References

Albrech, Steve, *Iconic Fraud Triangle Endures*, Fraud Magazine July/August 2014, Association of Certified Fraud Examiners

Fraud Risk Management Guide, Committee of Sponsoring Organisations of the Treadway Commission (COSO), September 2016

Internal Control – Integrated Framework, Committee of Sponsoring Organisations of the Treadway Commission (COSO), May 2013

Report to the nations on Occupational Fraud and Abuse 2016 Global Fraud Survey, Association of Certified Fraud Examiners [website], 2016 http://www.acfe.com/rttn2016/costs.aspx (accessed 7 January 2017)

Purpose of White Papers

A White Paper is an authoritative report or guide that informs readers concisely about a complex issue and presents the issuing body's philosophy on the matter. It is meant to help readers understand an issue, solve a problem, or make a decision.

5. Authors Biography

This White Paper written by:

Barry Davidow
B.Com, B.Acc, M.TaxLaw, ACA, CFE, CRMA, PFIIA, Advanced Diploma of Government (Management), Diplomas in Risk Management and Business Continuity, Government (Fraud Control), Government (Investigation) and International Financial Management

Barry is a Director of Fraud Prevention & Governance Pty Ltd and has over 20 years of experience in internal audit, fraud and corruption control, investigations, governance and compliance. He has contributed to books on fraud control, computer fraud, communications and sociology.

Matthew Lyon
B.Comm, CPA, MIAA,

Matthew has been involved in internal audit for 10 years in the NSW Government. Prior to this he was Financial Accountant for Catholic Education Office Parramatta. He spent 15 years with the Audit Office of NSW, the last four as engagement manager. He has also served in a number of charities and the Wollongong Council Audit and Finance Committee.

6. About the Institute of Internal Auditors–Australia

The Institute of Internal Auditors (IIA) is the global professional association for Internal Auditors, with global headquarters in the USA and affiliated Institutes and Chapters throughout the world including Australia.

As the chief advocate of the Internal Audit profession, the IIA serves as the profession's international standard-setter, sole provider of globally accepted internal auditing certifications, and principal researcher and educator.

The IIA sets the bar for Internal Audit integrity and professionalism around the world with its 'International Professional Practices Framework' (IPPF), a collection of guidance that includes the 'International Standards for the Professional Practice of Internal Auditing' and the 'Code of Ethics'.

The IPPF provides a globally accepted rigorous basis for the operation of an Internal Audit function. Procedures for the mandatory provisions require public exposure and formal consideration of comments received from IIA members and non-members alike. The standards development process is supervised by an independent body, the IPPF Oversight Council of the IIA, which is appointed by the IIA–Global Board of Directors and comprises persons representing stakeholders such as boards, management, public and private sector auditors, regulators and government authorities, investors, international organisations, and members specifically selected by the IIA–Global Board of Directors.

The IIA–Australia ensures its members and the profession as a whole are well-represented with decision-makers and influencers, and is extensively represented on a number of global committees and prominent working groups in Australia and internationally.

The IIA was established in 1941 and now has more than 180,000 members from 190 countries with hundreds of local area Chapters. Generally, members work in internal auditing, risk management, governance, internal control, information technology audit, education, and security.

Historians have traced the roots of internal auditing to centuries BC, as merchants verified receipts for grain brought to market. The real growth of the profession occurred in the 19th and 20th centuries with the expansion of corporate business. Demand grew for systems of control in companies conducting operations in many locations and employing thousands of people. Many people associate the genesis of modern internal auditing with the establishment of the Institute of Internal Auditors.

7. Copyright

This White Paper contains a variety of copyright material. Some of this is the intellectual property of the author, some is owned by the Institute of Internal Auditors–Global or the Institute of Internal Auditors–Australia. Some material is owned by others which is shown through attribution and referencing. Some material is in the public domain. Except for material which is unambiguously and unarguably in the public domain, only material owned by the Institute of Internal Auditors–Australia–Global and the Institute of Internal Auditors–Australia, and so indicated, may be copied, provided that textual and graphical content are not altered and the source is acknowledged. The Institute of Internal Auditors–Australia reserves the right to revoke that permission at any time. Permission is not given for any commercial use or sale of the material.

8. Disclaimer

Whilst the Institute of Internal Auditors–Australia has attempted to ensure the information in this White Paper is as accurate as possible, the information is for personal and educational use only, and is provided in good faith without any express or implied warranty. There is no guarantee given to the accuracy or currency of information contained in this White Paper. The Institute of Internal Auditors–Australia does not accept responsibility for any loss or damage occasioned by use of the information contained in this White Paper.