

www.pwc.com.au

Fraud Risk Assessment...in Practice

*Institute of
Internal Auditors
– Australia*

May 2013



pwc



Steve Hipkin

Director – Forensic Services, PwC

Leader of Brisbane Forensics

stephen.hipkin@au.pwc.com (07 3257 5154)

Background

- PwC Brisbane 2012-present
- PwC Indonesia 2009-12
- PwC Sydney 2005-09'
- Virgin Mobile Australia
- Vodafone Australia
- British Telecom
- London Metropolitan Police.

Agenda

1. Introduction
2. Inherent fraud risks?
3. Why conduct a Fraud Risk Assessment?
4. Case studies
5. Scoping
6. Data requests
7. Risk storm meetings
8. Preparation of a “Heat Map”
9. Maturity Benchmarking and next steps
10. Prize draw.

Why conduct a Fraud Risk Assessment?

- Cliché fraud scenarios
- “You don’t know what you don’t know”
- Proactive or Reactive?
- Operational impact of fraud
- Corporate credibility.

Case study 1

Preferential treatment to a national sports team

- A national sporting team used local council facilities for training and match days (under a partial sponsorship agreement)
- Whistleblower allegations that favourable hire rates were being offered, food and beverage sales were not correctly accounted for, and other service costs were being “written off”
- Furthermore, the Centre Manager was an Officer of the sporting team, and had a Conflict of Interest.

CS1 – Preferential treatment to sports team

Issues and process

- Potential fraud had previously been investigated, and a report sent to Government regulator
- Regulator had returned report, requesting additional and more detailed investigations
- Whistleblower evidence lacked integrity
- Council policies and procedures in relation to the sponsorship and employee responsibilities was vague and ambiguous.

Case study 2

Payroll fraud

- A company of 70 staff and 5 executives
- Payroll data is prepared for the staff and then sent to CFO, who adds exec details
- Information is then batched, signed off and sent to payroll run
- CFO had added an extra exec, and had “salary” paid to his own bank account
- This was not picked up for seven years. Losses were significant (\$1m plus)

CS2 – Payroll fraud

Issues and process

- Period of losses
- Ease of perpetration
- Lack of “real time” monitoring
- Segregation of duties
- Where else is there fraud risk?

Case studies – Outcomes

	Issues	Resolution	Success
Sports team	Ambiguous policies and procedures Unreliable whistleblower Heavy expectations from Regulator	Re-quantification of losses Employees and witnesses interviewed Report submitted (through Council) to Regulator	90%
Payroll fraud	Ease of fraud Age of Investigation Poor governance	Investigated Employee retired Funds “chased” but not recovered Process changed...after the horse had bolted	10%

Does an entity have a robust fraud management control framework?....ask yourself 12 questions

1. Have you developed a Fraud and Corruption Control Plan?
2. Is your fraud and corruption control function adequately resourced?
3. Is your SMT sufficiently knowledgeable and aware of the risks from fraud and corruption?
4. Are high risk business processes subjected to a rigorous system of internal controls?
5. How detailed and widespread is employee/supplier due diligence?
6. Are systems in place to detect fraud and corruption as soon as it has occurred?
7. Is it easy for employees to reports potential incidents of fraud and corruption?
8. Do adequate fraud and corruption policies/procedures exist?
9. Are suitably qualified internal/external investigative resources available?
10. Is an adequate fraud reporting (and escalation) process in place?
11. Do HR have clear and relevant guidelines regarding fraud and corruption management?
12. Does a post incident review always take place?

Scoping a Fraud Risk Assessment

Factors to consider:

1. It's like cricket....Test Match, One Day or 20-20....different, but the same!
2. It is essential to obtain “umbrella” coverage....high level/wide breadth is better than specific deep dive.
3. Offer to “test” controls at your peril
 - a. Misguided criteria
 - b. Time and cost.
4. One-to-one meetings or group workshops?
5. Maturity benchmarking
 - a. AS8001
 - b. ANO guidelines
 - c. CMC guidelines
 - d. a mixture.

AS 8001

Planning and resources

1. Fraud and corruption control planning
2. Review of the FCCP
3. Fraud and corruption control resources
4. IA activity in the control of fraud and corruption.

Prevention

1. Implementing and maintaining an integrity framework
2. Senior management commitment to controlling the risks of fraud and corruption
3. Line management accountability
4. Internal control
5. Assessing fraud and corruption risk
6. Communication and awareness
7. Employment screening
8. Suppliers and customer vetting
9. Controlling the risk of corruption.

AS 8001 (cont'd)

Detection

1. Implementing a fraud and corruption detection programme
2. Role of the external auditor in the detection of fraud
3. Avenue for reporting suspected incidents.

Response

1. Policies and procedures
2. Investigation
3. Internal reporting and escalation
4. Disciplinary procedures
5. External reporting
6. Civil action for recovery of losses
7. Review of internal controls
8. Fidelity insurance.

FRA – Typical document request

1. Organisation chart
2. Fraud and Corruption Policy
3. Fraud and Corruption Control Plan
4. *Public Interest Disclosure Policy*
5. Conflicts of Interest Policy
6. Role of the Fraud Control Officer
7. Fraud training materials
8. Training material on the Code of Conduct
9. Fraud risk register and incident register.
10. Code of Conduct/Values document
11. Example of the internal fraud investigations report/any internal fraud investigation report from the past 12 months
12. Data analytics tests conducted
13. Employment procedures or checklists (eg pre-employment process, new starter process, exiting employee process)
14. Supplier vetting procedures/Procurement Policy
15. CEO statement on fraud on corruption
16. Gifts register/No Bribes Policy
17. Fidelity Guarantee Insurance Policy.

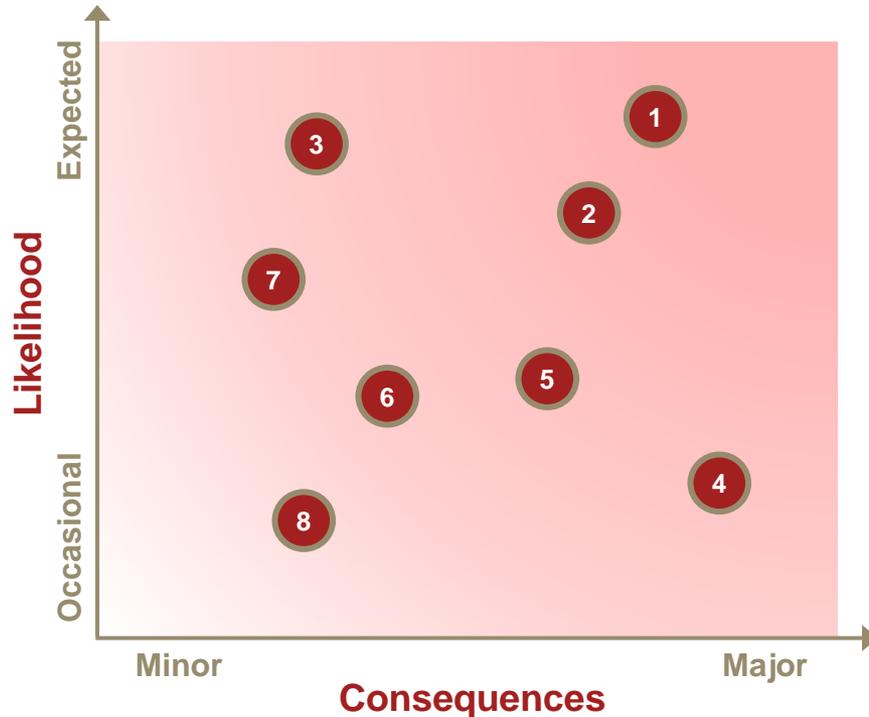
“Risk storm” meeting – Agenda (1-2 hrs)

1. Introduction and background
2. Fraud and Corruption – Definition
3. Inherent fraud risks – Three highest
4. Significant areas of fraud risk
 - a. Business Systems/IT
 - b. Sales
 - c. Contact Centre
 - d. Human Resources
 - e. Marketing
 - f. Finance/Admin.
5. Awareness and Communication
6. Information Security
7. Whistleblowing line
8. Draft Heat Map
9. Summary/next steps.

Proactive measures to prevent, deter and detect internal fraud schemes

- Fraud Awareness
- Pre-employment screening
- Whistleblower
- Fraud Risk Management
- Investigative intel and analysis
- STA (Suspicious Transactions Analysis)
- Cyber crime controls
- Management of Intellectual Property.

The heat map



Bribery and corruption

Due to significant (value and frequency) financial and business transactions with third party providers in high risk overseas destinations, a risk exists that senior employees may be vulnerable to allegations of bribery and corruption.

Vendor management

There is a risk of fraud around the vendor selection process, and payment for services which may or may not have been performed or completed in a substandard manner.

Financial management

There are multiple risks around the financial systems including the risk of duplicate payments, payments to unauthorised recipients, split orders to subvert delegated authorities and weak segregation of duties.

Human resources

There are a number of potential fraud risks including; paying phantom employees, weak segregation of duties and lack of detailed validation prior to approval of pay runs.

IT security

There is a risk that IT systems are vulnerable to unauthorised external penetration and confidential data could be removed without authority.

Sales

A risk of fraud exists due to; collusion between staff and agents, falsified commission claims, heightened by poor segregation of duties.

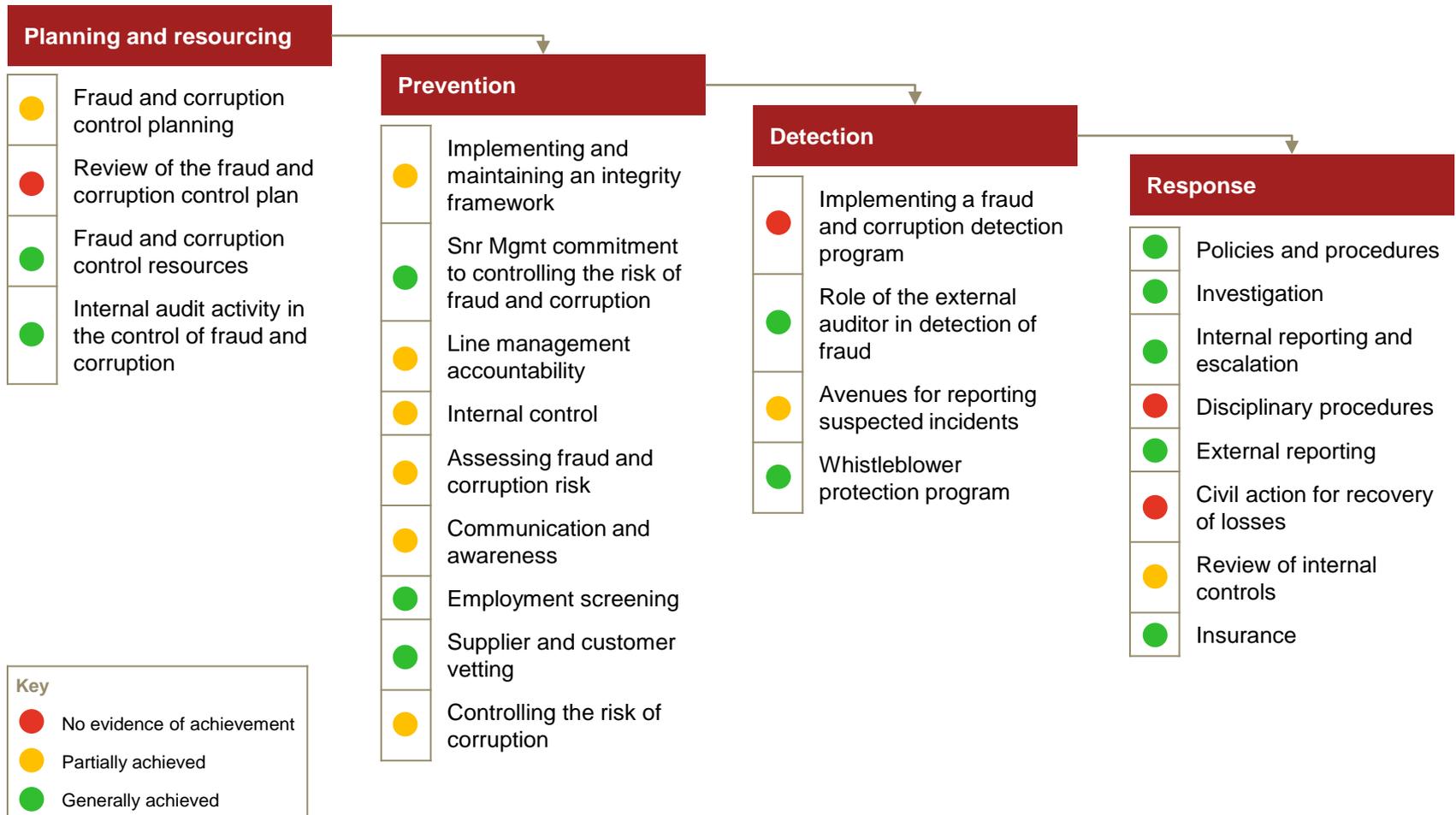
Intellectual property

A risk of fraud exists as a result of collusion between employees and third parties to disclose without authority strategic business information.

Underwriting

There is a risk of fraud due to collusion between employees, brokers and customers, the misrepresentation of insurance risk, and staff acting outside levels of authority.

High level comparison of company xyz against Australian standard for fraud and corruption control (AS8001)



Fraud and corruption...what are the emerging risks...what are the proactive solutions?

Emerging risks

- Procurement fraud
- Cyber-crime
- Theft of intellectual property
- Large project fraud
- Contractor performance
- Sustainability fraud
- Workplace bullying and harassment
- Misuse of regulatory reporting
- Professional negligence.

Proactive solutions

- Fraud Risk Assessment
- Fraud and Corruption Control Plan
- Planned data analytics
- Fraud awareness training
- A focus on culture (tone from the top)
- Strong compliance framework.

www.pwc.com.au

© 2013 PricewaterhouseCoopers. All rights reserved.

PwC refers to the Australian member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

Liability is limited by the Accountant's Scheme under the Professional Standards Legislation.

PwC Australia helps organisations and individuals create the value they're looking for. We're a member of the PwC network of firms in 158 countries with close to 169,000 people. We're committed to delivering quality in assurance, tax and advisory services. Tell us what matters to you and find out more by visiting us at www.pwc.com.au

WL127003973