www.pwc.com.au

Fraud Risk Management

"Fraud Risk Assessments"

LGMA Qld Governance and Corporate Planning Village Forum

March 2015

pwc

Agenda

- Introductions
- Fraud Risk Management
- Fraud Statistics – PwC's Global Economic Crime Survey 2014
- Fraud Risk Assessment
- Enterprise Wide Fraud Risk Assessment
- Case Studies

Fraud Risk Management

Fraud may be defined as “dishonestly obtaining a benefit by deception or other means”. This includes behaviour such as theft, providing false information, corruption, bribery or abuse of office.

Custodians of public funds and other people’s money must take their responsibilities seriously and ensure suitable procedures are in place to deter misuse of funds and guard against fraud.

Fraud can occur when least expected. It can be disruptive to the daily activity and morale of Councils, as well as clients and staff and can be devastating both from a financial and reputational perspective.

Fraud Risk Management - PwC's 2014 Economic Crime Survey 2014

- Results of the recent 2014 Economic Crime Survey show there are often a number of economic crimes that are occurring with increasing volume, frequency and sophistication.
- The Big 5:

- **Procurement**
- **Cybercrime**
- **Asset misappropriation**
- **Bribery and corruption**
- **Accounting Fraud**

Fraud Risk Management

- While there is a no foolproof method in preventing fraud and corruption, the risk can be minimised by taking a proactive, systematic approach to its management.
- As fraud negatively impacts on Councils in many ways – financial, reputational, and through psychological and social implications – it is important for Councils to have a strong fraud program that includes awareness, prevention and detection programs, as well as a ***fraud risk assessment process*** to identify risks within Council.
- Important to set the right tone from the top and ensure that Executives and staff understand their particular fraud risks and profile and that these risks are on the radar and treated seriously.

Fraud Risk Assessment (FRA) - Overview

- A fraud risk assessment (FRA) is often a critical component to Council's larger enterprise wide risk management framework. It helps to:
  - Identify current and emerging risks and implement enhanced controls.
- An important role of management is to provide oversight for the completion of an FRA so that management has a better understanding of fraud risks and the controls in place to mitigate those risks
- An FRA assists management and internal auditors in systematically identifying where and how fraud may occur and who may be in a position to commit fraud
- Councils need to reach their own conclusion with respect to the cost of controlling a risk compared to the benefits of mitigating or eliminating that risk.

Fraud Risk Assessment (FRA) - Types

Three types of common fraud assessments:

1. **Enterprise Wide Fraud Risk Assessment -** provides a comprehensive identification of fraudulent activities facing an organisation. Focuses on the internal control environment for assessing the likelihood of the risk occurring

2. **Business process fraud risk assessment -** designed to identify specific fraud threats at the business process level and link the specific internal control procedures to the fraud risk inherent to the process. Focuses on internal control procedures, monitoring controls and the information and communication controls

3. **Fraud prevention assessment –** designed to identify the most likely location of a fraudulent transaction in a specific account, transaction type and business location.

Enterprise Fraud Risk Assessment - Key steps

A **fraud risk assessment** generally includes the following key steps:

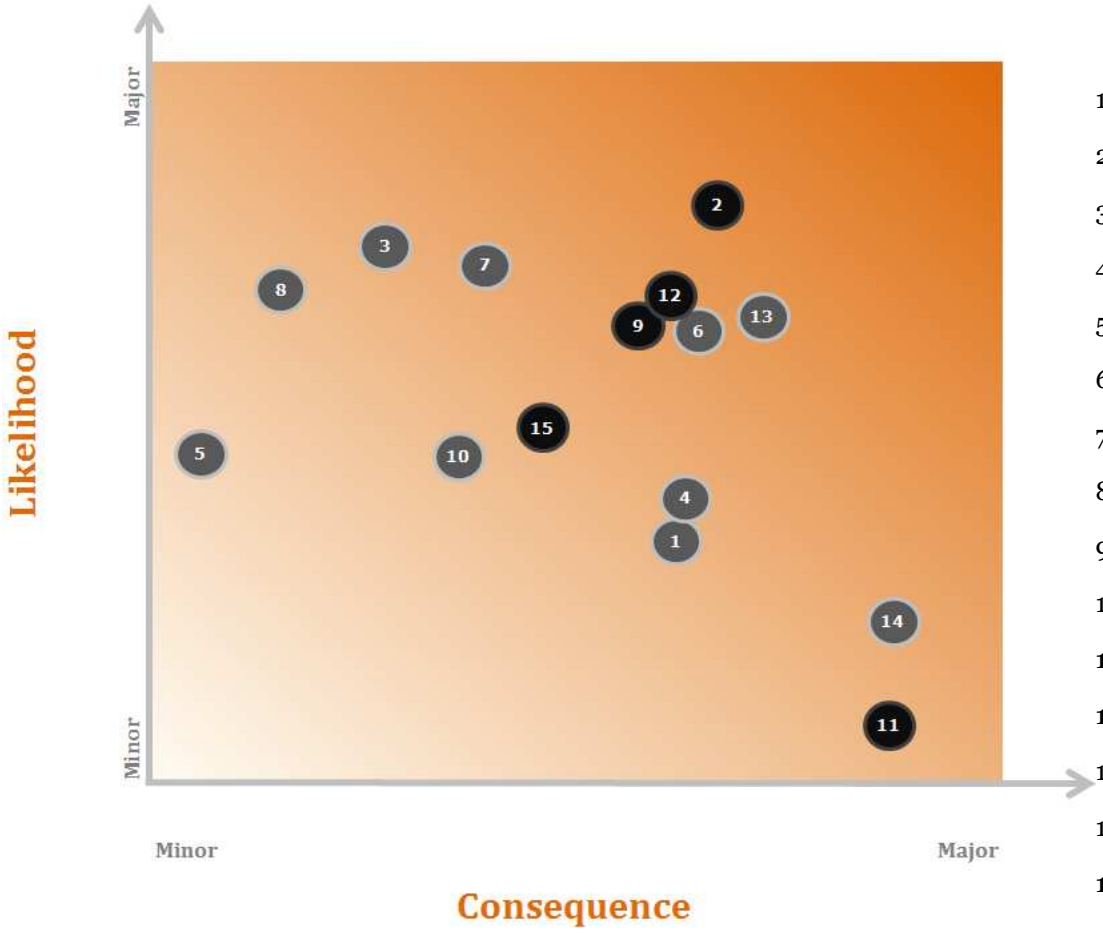
1. Identify relevant fraud risk factors – fraud risks to which operations are exposed
2. Identify potential fraud threats and prioritise them based on risk (i.e. evaluating risks for significance and likelihood of occurrence)
3. Map existing controls to potential fraud threats and identify gaps – identify and evaluate controls (if any) in place to mitigate key risks
4. Document and report the fraud risk assessment

Fraud risk assessments should be followed by the development of a fraud control plan, including nominating a person responsible for addressing the risk, implementing systems to address the risk, and considering alternative controls to mitigate the risks

Fraud Risk Assessment - How to approach?

1. Review key policies and procedures in place for fraud management
2. One on One meetings with management/senior executives (fraud risk focus and "buy in")
3. Conduct "risk storm" workshops with a wide cross section of Council employees, to discuss and identify fraud risk and complete the fraud risk assessment
4. Develop a **"Heat Map"** of inherent fraud risk, based on the outcomes of the meetings and workshops
5. Consider current and emerging risks and level of assurance in place throughout Council (3 lines of defence)

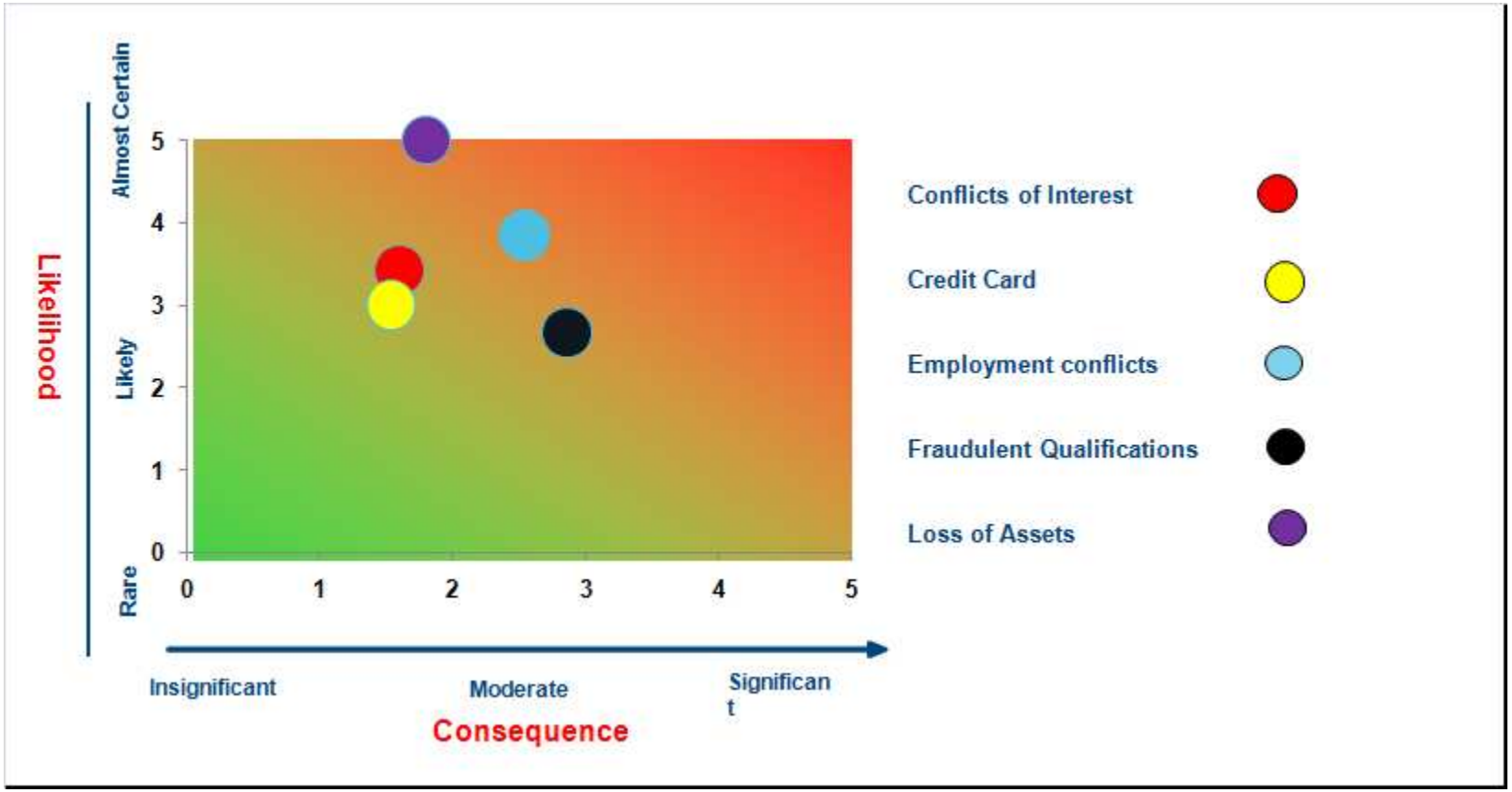
Fraud Risk Assessment – Example Heat Map – Current and emerging fraud risk



1. Land disposals/Acquisitions
2. **Contractor performance**
3. Conflicts of Interest
4. Contract tendering
5. Insurance claims
6. Loss/misuse of resources/procurement
7. Cash handling
8. Payroll
9. **Professional negligence**
10. Finance related fraud
11. **Technology/IP related fraud**
12. **Bank guarantee fraud**
13. Abuse of private/public partnerships
14. Capital infrastructure management
15. **Regulatory reporting misuse**

Fraud Risk Assessment – Example Heat Map

This chart shows the risk assessment of 5 key areas, considered fraud threats by workshop participants.



Fraud Risk Assessment - Summary

- ✓ Adopt a thorough fraud risk assessment to identify a range of risks
- ✓ Address identified risks by corresponding fraud prevention plan strategies
- ✓ Consider the level of assurance coverage throughout Council (3 lines of defence)
- ✓ Update and review fraud assessments with any change in the business, such as the addition of a new structure or business unit, deployment of a new program, heightened risk or change in incident levels

Case Study One:

Industry: National Healthcare Company

Financial impact: $400,000

Details:

- Male IT engineer
- 7 fictitious vendors, 25 corporate credit card transactions and 146 false invoices

Cause:

- Failure to adequately identify fraud risks and mitigate
  - **Vendor due diligence**
    - False ABNs /legitimate ABNs of different companies
  - **IT security**
    - Utilised access to three Regional Managers email accounts to send 50% of the invoices to accounts payable.

Case Study Two:

Industry: International Mining and Construction Company

Financial impact: $550,000

Details:

- Female procurement employee
- 3 legitimate + 3 fictitious vendors, 58 false invoices

Cause:

- Failure to adequately identify fraud risks and mitigate
  - **Employee screening and due diligence**
    - 10 year history of fraud related offences
  - **Procure to pay system controls**
    - No approval process or workflow governing changes to vendor bank account details / system audit trail able to be switched on and off by all users / no email notification or reporting of bank account changes

Any Questions?