Ivan Pranjić
Fraud Prevention, Detection and Investigation

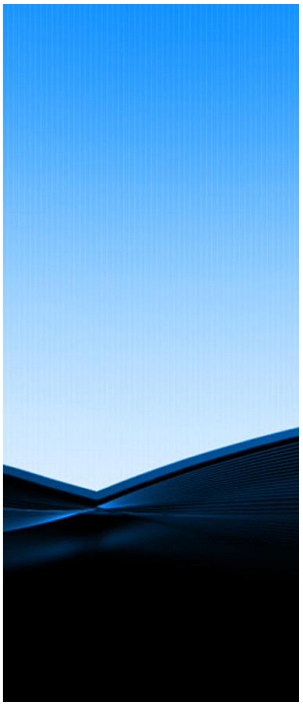
1

Contents

- Fraud risk management
- Fraud prevention techniques
- Proactive fraud detection
- Effective fraud investigation
- Electronic investigation
- Financial statement interpretation

2

How to establish a robust framework?



Fraud risk management framework should include:

- **Identify areas of high risk**
- **Assess the risk**
- **Involve all staff**

3

Common risk areas

Six key areas of risk apply to most organisations:

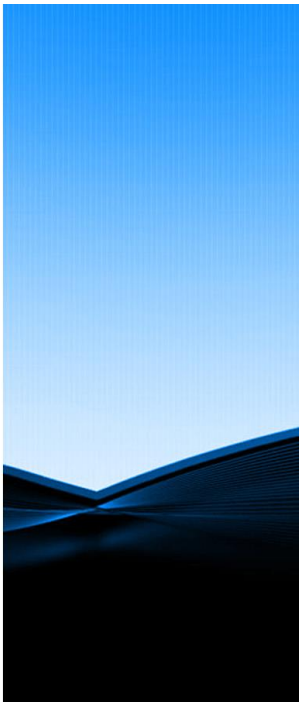
- Purchasing and payroll
- Sales and inventory
- Cash and cheques
- Physical security
- Piracy, intellectual property and confidental information
- Information technology

4

Some easy to implement fraud prevention techniques!

There are four key elements to effective fraud prevention:

- Oversight by the board and audit committee
- Policies and training
- Employment screening
- Internal fraud controls



5

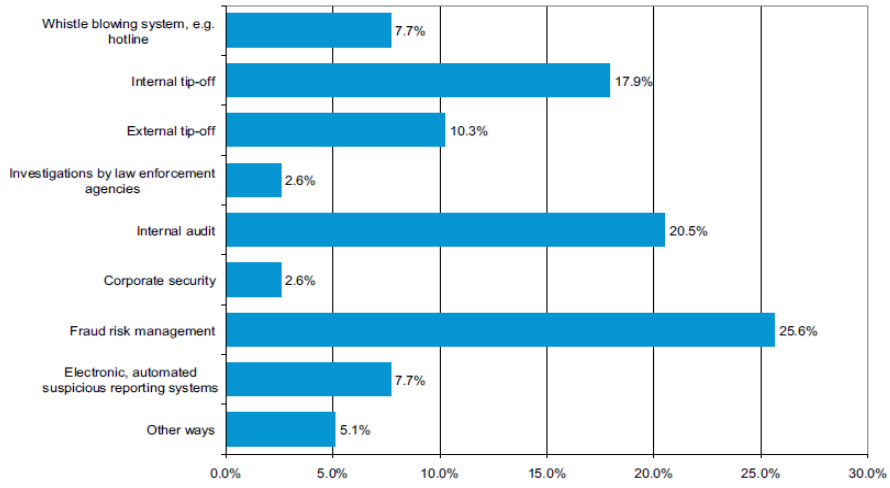
Fraud prevention techniques

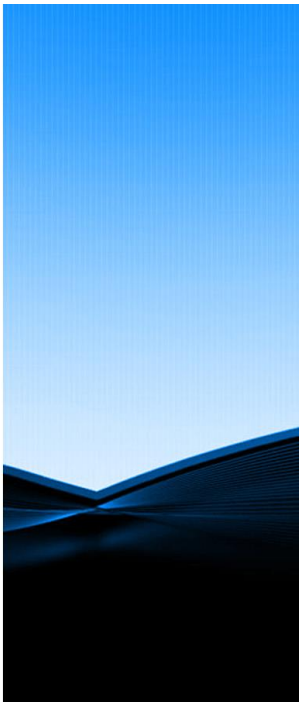
Basic fraud control and prevention techniques:

- Staff selection tests **75,0%**
- Whistle blowing **68,3%**
- Compliance program **78,8%**
- Consultation on fraud prevention **53,8%**
- Internal audit **86,5%**
- External audit **93,3%**
- Internal controls **94,2%**
- Corporate security **52,9%**
- Specific fraud training **36,5%**
- Code of Conduct **87,5%**

6

Making fraud detection part of business as usual!





7

Protected disclosures / whistleblowing

Whistleblower program should be designed to:

- Encourage the reporting of incidents of fraud, corruption, legal or regulatory non-compliance and questionable accounting
- Allow for the effective and efficient investigation disclosures
- Protect those making the disclosure from reprisal
- Appropriately manage those subject to an allegation

8

Protected disclosures / whistleblowing

Effective whistleblower program has four elements:

- Develop a whistleblower protection policy and procedures
- Develop a disclosures database
- Implement methods of receiving disclosures
- Communicate and train

9

Automated detection programs

An automated fraud detection can search through millions of transactions to identify ones which might be worth a closer look.

Some of more useful tests are as follows:

- Employee and payroll test
- Purchasing and payment test
- Customers and sales test

10

Effective fraud investigation!

Fraud investigation resources generally fall into four categories or skill-sets. In majority of cases, most if not all of them are required to fully investigate a suspected fraud. These skills are illustrated and described

11

Responding to a fraud incident

The following plan is a guide to the actions that should be taken in the event that a fraud incident occurs or a suspicion of fraud arises.

Before you start:

- Obtain as much information as possible before anyone is questioned, confronted and interviewed
- To be aware that fraud is frequently large scale and international
- Crucial to the eventual outcome of an investigation

12

Responding to a fraud incident

Fraud investigation is by necessity a confidential task and is a sensitive matter for the vast majority of organisations.

Fraud must be treated seriously and that responsibility for handling fraud incident is assigned to senior, trusted individual, most commonly:

- Security advisor
- Internal audit manager
- Risk manager
- Compliance officer

13

Responding to a fraud incident

Should be done when fraud suspicion is received:

- Alert fraud incident manager that allegation exists
- Obtain as much detail about the allegation as possible
- Be careful not to alert the suspect from the allegation
- List all possible circumstances surrounding the allegation
- Maintain a log of all actions taken by investigators
- Prepare accurate file notes of all evidences

14

Responding to a fraud incident

Current employee

- Full background check
- Office and computer search
- Calls and emails analysis
- Forensic accounting
- Surveillance of suspect
- Forensics examination

Third party, supplier, customer

- Full background check
- Detailed forensic examination
- Surveillance of suspect
- Document forensics
- Statements or other information from third parties

15

Responding to a fraud incident

Suspect interviews

- Many investigations conclude with formal interview with the suspect(s), during which all evidence will be out to suspect under controlled conditions
- In most cases, interviews should only be conducted once all investigations are complete
- Legal advice should be sought before interviews are conducted unless using trained, specialist investigator

16

Responding to a fraud incident

Reporting of investigation findings and subsequent actions

Armed with evidence gathered from the undertaken investigation the incident controller should obtain legal advice as to the appropriate way forward. Conclusions could be:

- **The evidence is insufficient or inconclusive**
- **The evidence is strong but requires further support**
- **The evidence is conclusive**

17

Responding to a fraud incident

Legal actions and police referral

Likely legal actions against suspects in fraud matter include the following:

- Civil action for recovery of defrauded funds, losses and damages
- Alternatively, you may prefer to alert the police who will consider your claims and evidence before deciding whether to pursue the matter in the criminal area

18

Responding to a fraud incident

Personnel management and public announcements

An important aspect of fraud incident planning involves the internal and external management of the incident

- Rather then avoiding comment on the matter, or relying on office rumor, it is better to officially notify staff that an investigation has been conducted
- It is useful to have a prepared plan should the matter become public knowledge through the press or court announcements

19

What if there's no paper trail?

- Traditionally the collection of evidence in fraud investigation has relied upon the presence of a physical paper trail
- Computer forensics is a seizure and analysis of electronic data
- Computer forensics is an integral part of modern fraud investigation

20

Electronic investigation

The forensic image process

- The fundamental principle of computer forensics is that original data is ***never*** altered
- For this reason, forensics software is used to take an exact copy of a ***target*** computer system
- This ensures both integrity of the target system and the integrity of evidence. Technicians must be able to justify their actions in future court proceedings

21

Electronic investigation

Data analysis

A computer forensic technician will examine the entire structure of a hard disk, looking to collect all possible evidence. On examination such information can be located as:

- **File slack**
- **Data fragments**
- **System slack**

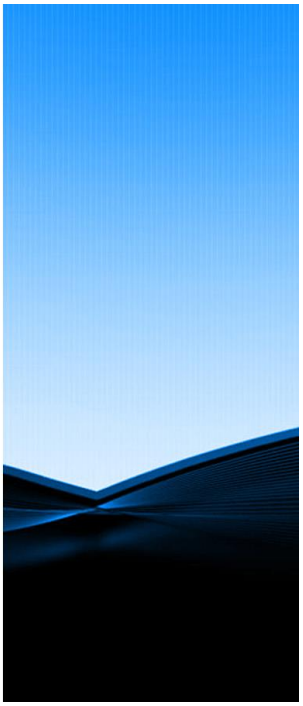
22

Do your numbers lie?

Forensic accounting is a discipline that arose to deal with instances of financial misstatement.

Financial accountants are used in two ways:

- To investigate general weaknesses
- To investigate specific situation



23

Financial statement misrepresentation

High risk areas for misstatement

Primary reasons for misstatement of financial accounts, due to error or accounting irregularity:

- Revenue recognition
- Expense understatement
- Asset overstatement
- Understatement of liabilities or asset impairment
- Inventory variances

24

25