Faculty of Business
School of Accountancy
BSB213 Governance Issues in E-Business

Lecture 10/Workshop 10 Outline
Monitoring & evaluation of IT performance
Fraud prevention and detection

Topic Outline:

- ME1 Monitor and evaluate performance
- Defining fraud
- Dealing with fraud
- Detecting and preventing fraud
- Computer security

Prescribed Reading:

- COBIT 4.1 pp153-156

Recommended Reading:

- None (but see below)

Workshop Questions

These questions should be prepared for the next workshop to assist with your understanding of fraud issues.

1. Research Article

Hormazi, A.M. and Giles, S. (2004) "Data Mining: A competitive weapon for Banking and Retail Industries" Information Systems Management Vol 21, No. 2 p62-71. Available from Library databases, Proquest Direct.

Present a summary of this article and its relevance to monitoring and IT Governance.

- This article defines data mining and identifies and covers the operations of data mining.
- The article is from Spring 2004 of Information Systems Management
- Increase in amount of data collected is one reason to look to mining. But also declining cost of data storage and increasing ease of collecting data, development of robust and efficient learning algorithms to process data, and declining cost of computational power. Offers a new way of doing business.
- Central idea to data mining: to extract important information from existing data and enable better decision making throughout an organisation.
- Can improve decision making but also reduce information overload.
- Operations include:

- Clustering/segmentation (grouping data into clusters sharing patterns/characteristics)
- Visualisation (graphical representation of data)
- Predictive modelling (predicting a specific attribute basd on other attributes in the data)
- Link analysis (Includes three specialisations: associations discovery, sequential pattern discovery, similar time sequence discovery)
- Deviation detection (Deviation detection – outliers express deviation from expectation – includes fraud detection).
- Dependency modelling (Significant dependencies among variables existing at two levels – structured and quantitative (locally dependent versus strength of dependency using a numerical ascale).
- Data Summarisation (summary about a subset of data).

- Identifies practical uses including analysing medical outcomes, detecting credit card fraud, predicting customer purchase behaviour, predicting personal interests of web users, and optimising manufacturing processes.
- Article then goes on to focus on marketing, risk management, fraud detection, and customer acquisition and retention.
- ***Marketing*** essentially is looking to target the right customers with our marketing activities.
- ***Risk Management*** is looking to cover risks involving insurance but also business risks arising from competitive threat, poor product quality and customer attrition.
- ***Fraud Detection*** is looking to detect fraudulent actions with a model built using fraudulent behaviour done in the past and use this to identify behaviour that is similar.
- ***Customer acquisition and retention*** is looking for customers that potentially we can acquire, and then ones that may be fleeing us so we can give them special love to stay with us.
- Article then examines the banking industry. Gives solid examples around each activity supported by data mining that is the focus of the article. **Note Falcon and my recent anecdote about Yahoo.**
- Article then examines the retail industry and each activity in focus. Emphasis here is less on fraud detection than the banking sector, more focus on marketing.
- **Implications for IT Governance:**
  - Use of automated detection systems for fraud detection and outlining in particular.
  - Could be used to detect fraudulent behaviour passively rather than actively (cfr WorldCom example in Workshop 11).
  - Could build up a library of conditions and monitor for those breaches.
  - Also recall – for brownie points – the fact that governance also requires the board to consider items of value for the business, not just risk – so if there is an opportunity to create value then the board needs to consider it.

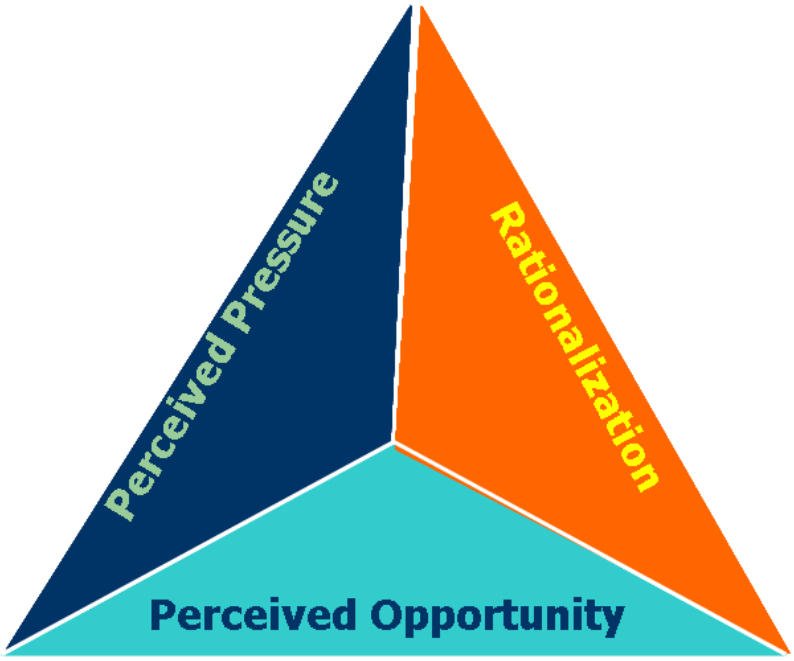
2. Research Case

a. Wells, J.T. (2004) "The Quarter-Million-Dollar Caper" Journal of Accountancy Vol 198 No.5 p89-91. Available on Proquest Direct.

b. Peterson Kramer, B.K. & Buckhoff, T.A. (2005) "Catching Fraudsters with their hands in the Till" The CPA Journal, Vol 75 No.5 p13-15. Available on Proquest Direct.

Analyse these cases and present how they link to the fraud triangle and symptoms of fraud outlined in the lecture slides. What were the key causes of these frauds?

- The fraud triangle, recall, is:



- Symptoms of fraud are:
  - Accounting anomalies
  - Internal control weaknesses
  - Analytical anomalies
  - Extravagant lifestyle
  - Tips & complaints
  - Unusual behaviour
- For the first case (quarter-million dollar caper) we can note:
  - Perceived pressure: Need to keep 90-day receivables high to keep the line of credit.
  - Rationalisation: "Knew the two customers would pay, so couldn't see the problem" Victimless 'crime'.
  - Perceived Opportunity: Easily done. No-one would ever know.
- Symptoms:
  - Accounting anomalies:
  - Internal control weaknesses: Clerk could simply make the change without question.
  - Analytical anomalies: 90-days accounts receivable higher by $250,000 than sales.
  - Extravagant lifestyle
  - Tips & complaints
  - Unusual behaviour
- **Discuss: was it 'fair' to do what was done? Was it the right thing to do? Do you think Tim ever felt like he'd done something wrong?**
- For the second case (Cashier Supervisor):
  - Perceived pressure: Financial pressure.
  - Rationalisation: 'deserve it' in her poor personal situation. Also long service (but started after only two years in the role!).
  - Perceived Opportunity: Rarely audited. No-one checked on her. No-one suspected her. (it's always the receipts clerk or the payroll clerk – money coming in, money going out)

- Symptoms:
  - Accounting anomalies:
  - Internal control weaknesses: Rarely audited due to 'immateriality', despite increasing revenues. No independent checks on Debbie that would have ensured that all of the money collected, no prenumbering. No rotation of duties, no enforced leave.
  - Analytical anomalies: Expenses increasing faster than revenue.
  - Extravagant lifestyle: Horses out of town. Gifts for everyone?
  - Tips & complaints:
  - Unusual behaviour: always working when sick; never letting anyone do the job.
- **Discuss: Did she get her comeuppance? Discuss the fraud triangle – what controls should the business have put in place? Liability of past directors?**
- For the second case (Welfare eligibility examiner):
  - Perceived pressure: Owes parents money. No real money and looking after two kids on her own.
  - Rationalisation:
  - Perceived Opportunity: Never checked, no supervision. Can get away with it, got away with it before (probably why she got 40 years).
- Symptoms:
  - Accounting anomalies:
  - Internal control weaknesses: Little or no supervision. Irregular audit. Reference checking?
  - Analytical anomalies: Same po boxes for people ('Smith'?) – data mining would apply.
  - Extravagant lifestyle: Very generous with coworkers. Bought a microwave oven (who the heck does that?).
  - Tips & complaints:
  - Unusual behaviour: always nice – seriously, who is always that nice?
- **Discuss: Did Julie get more than she deserved (40 years? Ouch!). Recall differences in legal systems.**
- See the exhibit:

EXHIBIT

Summary of Red Flags Present in Each Case

Red Flags	Cashier Supervisor	Welfare Eligibility Examiner
Extravagant lifestyle	✔	✔
Poor or nonexistent internal controls	✔	✔
Inadequate segregation of duties	✔	✔
Independent checks on performance not conducted	✔	✔
Placing too much trust in key employees	✔	✔
Lack of prenumbered documents	✔	✔
No reconciliations	✔	✔
Background checks not conducted		✔
Lax management oversight	✔	✔
No use of sick leave/vacation time	✔	
Excessive hours worked	✔	
Inexplicable unprofitability/cash flow problems	✔	
Personal financial pressure (real or perceived)	✔	✔
Lack of supporting documentation	✔	✔
Understaffed internal audit department	✔	✔

- Schemes are simple and bound to be found out eventually.
- What kind of supervisor doesn't note that 97% of cash is stolen? Clearly someone who doesn't understand the business. Don't be that supervisor!
- Keep your eyes & ears open!

3. Research Issue

Research and present some information on the new types of fraud which are emerging (e.g. click fraud) and how these frauds are being detected.

New fraud:

- Click fraud – Increased sophistication on
- Telecommunications crime (especially VOIP) – use a landline!
- Identity theft (usually credit card; Google Alerts, education. Don't put up too much on Facebook!)
- Ponzi scheme – new investors pay outrageous returns to old investors until collapses in a heap – regulation and monitoring, but takes a long time.
- Online sharemarket manipulation ("pump and dump")
- False billing

Discuss ways of addressing each

4. Case 1 - Programmer Fraud

One day when the analyst-programmer was on holidays, the bank experienced a minor problem with its computer operations which required the Information Systems Manager to compare the current version transaction update program with the previous version to determine whether any recent amendments were the cause. In doing so, she stumbled on a line of code which referred to a personal cheque account number.

On further investigation, the manager established the following facts:

1. The account belonged to the senior analyst-programmer.
2. The purpose of the above program code was to prevent transactions from updating that account.
3. Details of the account were suppressed from all computer generated reports.
4. The total funds withdrawn from the account from its date of inception was $170,000.

From the information that was pieced together, it was apparent that a serious computer fraud had occurred over a period of 7 months. However, no balancing problems had been experienced in the bank's ledger or branch controls, nor was there any indication that other customer accounts had been affected.

Requirements:

1. Suggest possible control weaknesses that may have existed at the bank to allow such a fraud to be perpetrated and to go undetected for seven months.

    - Inappropriate authority to make changes to software
    - No peer review of software code
    - No software methodologies in place
    - No testing of software and reconciliation.

2. What auditing techniques may have been useful in detecting this fraud?

- Usually, would model the processes to be done on the same inputs and compare to the outputs – data mining.
- Configuration/change audits.

5. Case 2 - Seven Banners

Cathy looked over the personnel records for her employee Susan once more. Cathy had supervised Susan at Seven Banners amusement park in Surfers Paradise for eight months. Susan, a university student, had been a reliable and likeable employee at the park; she often worked at the gate admissions booth. But now Cathy worried that Susan might be stealing money from customers as they paid for their tickets.

In the last month, Cathy had noticed eight incidents where families were over-charged for admission – all alleged oversights by Susan. The most recent incident happened that morning. As Cathy made her usual rounds through the park, she was approached by a customer with a question about his tickets receipt. The customer had paid for his family's admission with a credit card and received a standard receipt showing the total price of $305.50 and his signature.

Seven Banners' admission prices were as follows:

Adult $43.50
Child $35.00

The customer explained that his family of seven – two adults and five children – should have only cost $262.00, indicating that he paid for one extra adult ticket. He also showed Cathy his family's seven ticket stubs.

Cathy walked the annoyed customer back to the park gates. The customer led Cathy to the booth where he paid – Susan's booth. At the sight of Cathy and the customer, Susan seemed agitated and caught off guard. Before Cathy could explain the situation, Susan blurted out to the customer, "I'm so glad you came back – I just realised that you were mistakenly overcharged. Let me credit your visa for that."

Back in her office, Cathy thought how it was strange that if Susan had made an honest mistake in overcharging the customer that she could have later recognised that specific error. Seven Banners used an electronic ticketing system; employees need only enter the number of adults and children. Then, the system automatically calculates the total price and prints the appropriate number of tickets. If Susan had mistakenly entered 3 adults instead of 2, the customer would have caught the mistake right away because he would have had too many tickets. Cathy also wondered about Susan's seemingly nervous behaviour.

In considering all of Susan's overcharge incidents, Cathy noticed some commonalities: they were all paid with credit cards, and they were all large families (at least seven people). Cathy suspected that Susan purposely charged large families an extra ticket and then kept it, selling it to a cash-paying customer later in the day and then pocketing the cash. Susan was banking on the hope that the large family would assume the inflated charge was correct since they would expect a large amount anyway. The five customers who caught the "mistake" were the only ones to double check the maths.

Cathy leaned back in her chair and sighed heavily. Through her window she could see the long lines of people waiting to get on Seven Banners' newest roller coaster ride. "How can I prove what I suspect?" Cathy wondered.

Requirements:

1. What methods can Cathy use to detect/investigate whether Susan is really committing fraud?

- Deductive would include – average sales per teller comparison; #sales per person; credit card sales compared to cash sales per teller.
- Audit trail review
- Whistleblowing/complaints line

- What are controls that Seven Banners could implement to prevent and detect this type of fraud in the future?

- Sequential ticket numbering;
- Independent head count at the turnstiles.
- Reconciliation of credit card and cash sales for the day to tickets sold (won't prevent it but highlights issues).

- Indicators:
  - Flat or declining revenue.
  - Increasing cost of sales.
  - Excessive or increasing inventory shrinkage.
  - Ratio of cash sales to credit card sales decreasing.
  - Ratio of cash sales to total sales decreasing.
  - Ratio of gross sales to net sales increasing.
  - Discrepancies between customer receipt and company receipt.
  - Customer complaints and inquiries.
  - Forged, missing or altered refund documents.