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

Lecture 11/Workshop 11 Outline
Monitoring the Processes – Fraud Prevention

Topic Outline:

- CobIT framework – M1 Monitoring the Processes
- Fraud prevention
- Reducing opportunities for fraud
- Common ways to commit revenue fraud
- Computer fraud & Internal controls
- Threats to EC Security
- Managing EC Security

Prescribed Reading:

- CobIT 4.1

Weekly Assignment Questions

1. **Research Articles**

- Lucas, P. (2005) "New Image for Check Fraud Prevention" Collections and Credit Risk Vol 10. No. 4 p16-18.

  Available from Proquest – *use "search for journals and magazines" to find the journal, then locate the issue (April 2005)*

  Float occurs when there is a delay in the clearing of payments between banks. It is most obvious in the time delay between a cheque being written and the funds to cover that cheque being deducted from the payer's account.

  Cheques are basically inherently risky. Speeding up the cheque processing using image processing.

  Check fraud costs $15bn annually. Mentions Wachovia – in the news lately in its merger with Wells Fargo, not CitiBank as touted by the Federal Reserve.

  Growing cost, need to be sure though the control doesn't cost more than the loss. Mentions PCI Standard – note that this is a 2005 article, well and truly in now.

  The quicker it's processed the harder it is for cheque fraud to occur.

  Notes ATM cheque fraud.

  Still fairly inaccurate – 60-70% accurate.

- Foote, K and Bange, R. (2006) "Fraud and corruption control" Find at http://www.cmc.qld.gov.au/data/portal/00000005/content/90949001129616149252.pdf

  Threats can be internal or external. Notes the existence of reputation risk.

CMC introduces 10-element model to combat fraud.

Cost in fraud is approximately $3bn per annum.

Majority of large fraud find is by employees. Poor internal controls is the largest underlying cause of fraud – recall the fraud triangle and the 'opportunity' element.

The ten elements of an effective fraud and corruption control plan are:

- *Agency wide integrated policy*
- *Risk assessment – see AS8001-2003*
- *Internal controls*
- *Internal reporting*
- *External reporting*
- *Public interest disclosures*
- *Investigations*
- *Code of conduct*
- *Staff education and awareness*
- *Client and community awareness*

- Case, G. L. "Fraud: How to Prevent It in Your Organization". Nonprofit World, May/June 2008. Available in Proquest. .

  Lose on average $100K per annum. This can be very bad for a NFP.

  Cash fraud includes:

  - *Theft of deposits*
  - *Counterfeit documents*
  - *Theft of receivables*
  - *Lapping*
  - *False credits and write-offs*
  - *Theft of non-cash items*
  - *Theft of cash received in direct-contact solicitations*

  Investment fraud:

  - *Stealing investments or diverting income or gains*
  - *Borrowing securities for personal use*
  - *Recording phony investments to window dress the FS*
  - *Misclassifications and misstatements*

  To prevent it:

  - *Be aware*
  - *Ensure the control of donor funds to meet the requirements of the donor*
  - *Keep good records*
  - *Establish controls over purchase and donation*
  - *Create controls*
  - *Maintain records of donor restrictions*
  - *Be sure to properly observe board instructions*

Read these 3 articles and present a summary of all their issues.

2. **Research Case**
Holtfreter, K. (2004) “Fraud in US Organisations: An examination of Control Mechanisms” Journal of Financial Crime Aug. Vol 12, No. 1 p88. See Proquest Direct.

Analyse the issues re fraud prevention identified in this article.

- *Screening – background checks for new employees as well as regular checks for current employees*
- *Internal and external audit function*
- *Whistleblower hotlines, particularly anonymous hotlines*
- *This paper presents the results of research to examine the effect of each control mechanism on fraud losses.*

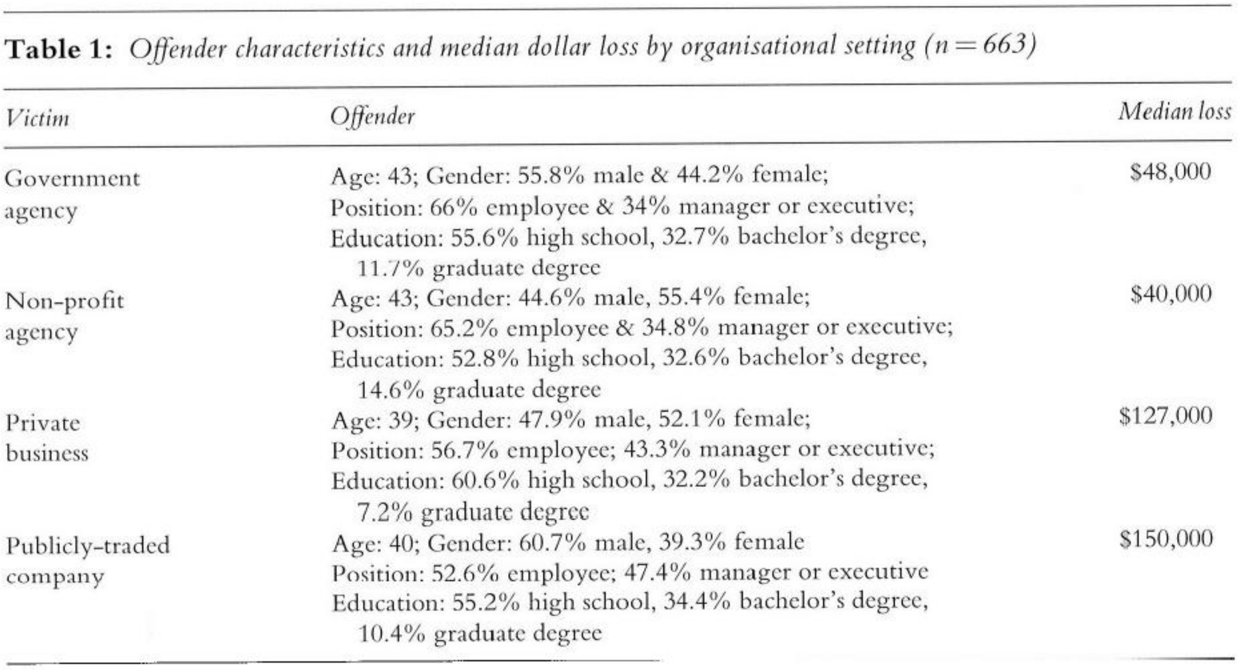

Table 1: *Offender characteristics and median dollar loss by organisational setting (n = 663)*

Victim	*Offender*	*Median loss*

Government agency	Age: 43; Gender: 55.8% male & 44.2% female;
	Position: 66% employee & 34% manager or executive;
	Education: 55.6% high school, 32.7% bachelor’s degree, 11.7% graduate degree
		$48,000

Non-profit agency	Age: 43; Gender: 44.6% male, 55.4% female;
	Position: 65.2% employee & 34.8% manager or executive;
	Education: 52.8% high school, 32.6% bachelor’s degree, 14.6% graduate degree
		$40,000

Private business	Age: 39; Gender: 47.9% male, 52.1% female;
	Position: 56.7% employee; 43.3% manager or executive;
	Education: 60.6% high school, 32.2% bachelor’s degree, 7.2% graduate degree
		$127,000

Publicly-traded company	Age: 40; Gender: 60.7% male, 39.3% female Position: 52.6% employee; 47.4% manager or executive Education: 55.2% high school, 34.4% bachelor’s degree, 10.4% graduate degree	$150,000

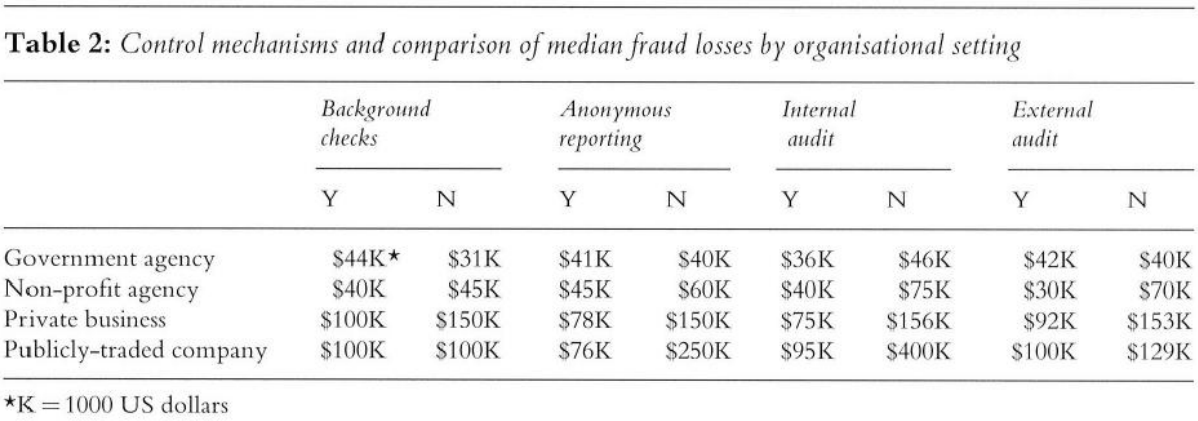

Table 2: *Control mechanisms and comparison of median fraud losses by organisational setting*

	Background checks		*Anonymous reporting*		*Internal audit*		*External audit*	
	Y	N	Y	N	Y	N	Y	N
Government agency	$44K*	$31K	$41K	$40K	$36K	$46K	$42K	$40K
Non-profit agency	$40K	$45K	$45K	$60K	$40K	$75K	$30K	$70K
Private business	$100K	$150K	$78K	$150K	$75K	$156K	$92K	$153K
Publicly-traded company	$100K	$100K	$76K	$250K	$95K	$400K	$100K	$129K

*K = 1000 US dollars

- *Anomalous results (e.g. background checks result in higher losses) are considered to be either discovery effects or that the check is not as effective. So background check won’t find a first-time offender.*
- *Discussion point – what is the most effective and why? Can you explain differences between organisational settings? Why wouldn’t you put these in place?*

3. **Research Issue**

Research how fraud of electronic business operations is being prevented?

For credit card transactions conducted in person, a system involving microchips and personal identification numbers (PINs) is currently being developed in the United Kingdom.

Chip and PIN cards have the potential at some point in the future to provide more secure transaction technology through the use of chip readers and PIN pads attached to computers. Not really available yet though.

Two additional online fraud prevention strategies have been developed in partnership with financial institutions and card issuers:

- *an address verification service (AVS); (verify address with the credit card provider) and*
- *a card verification number (CVN). (those extra three digits on the back).*

Payer authentication offered through both Mastercard ('Mastercard Securecode') and Visa ('Verified by VISA'). These are password-based programs which allow registered cardholders to verify their purchases by entering a password in a pop-up box on the computer screen when an online purchase is being made.

There has been the development of third-party provider web payment validation services (e.g. PayPal, Google Checkout).

Simple manual review techniques are also effective:

manual review techniques employed (in order of common use) were:

- *phoning the customer*
- *checking customer records*
- *emailing the customer*
- *phoning the bank*
- *checking a 'bad customer' database*

Development of systems like Falcon etc which is used to monitor by the banks to monitor transactions, together with teams of people devoted to keeping an eye on consumer credit card fraud.

See: Online credit card fraud against small businesses

Kate Charlton and Natalie Taylor
ISBN 0 642 53846 8 ; ISSN 1326-6004
Canberra: Australian Institute of Criminology: 2004

4. Case 1 - The Dude (Fraud Symptoms)

In his own words, Daniel Feussner was "The Dude". With his waist-long dreadlocks, part-time rock band, and well-paid job managing Microsoft's online search directory—he seemed to have it all. Originally from Germany, Feussner, now age 32, earned his doctorate and taught at the University of Munich before coming to the U.S.. where he started his career in computers. In 1996, Feussner started working with Microsoft as a director of operations for US-Speech Engineering Services and Retrieval Technology—working on a new, closely guarded search engine tied to the company's .NET concept.

Microsoft allows employees to order an unlimited amount of software and hardware, at no cost, for business purposes only. Between December year 2001 and November year 2002, Feussner ordered or used his assistant and other employees (including a high school intern) to order nearly 1700 pieces of software. He then resold them on the street for reduced prices—reaping more than $9 million. When items with a cost of goods sold of more than $1,000 are ordered, an e-mail is sent to the employee's direct supervisor, who must click on an "Approve" button before the order is filled. The loosely controlled internal ordering system reflects the trust the company has in its employees.

In June, FBI agents said they saw Feussner exchanging a large box of software for cash in a parking lot in Bellevue. The FBI contacted Microsoft security and began monitoring Feussner's bank accounts. Previously, one account with a major bank had an average balance of $2,159. In a short time, the average balance ballooned to $129,775. Another account showed irregular deposits totaling $500,000—none of which appeared to be from any legitimate income.

Investigators also noted that Feussner purchased a $95,000 Ferrari F355 Berlinetta, a $36,000 Jaguar XJ6 and traded in lesser vehicles for a $37,000 black 1995 Hummer, a Mercedes 500SEL, and a $21,900 Harley-Davidson. He also bought an $8,000 platinum diamond ring, a $2,230 Rolex wristwatch, and a $4,000 bracelet. For a relatively low-level manager Fuessner's lifestyle was impressive.

Steve Schnase, who lived across the street from Feussner, said his neighbour was clearly wealthy, but not flamboyant with his money. He described Feussner as an intelligent man who didn't flaunt his education, would loan neighbours tools and was always friendly. Schnase was surprised when he heard the accusations.

"The Dude" was fired from Microsoft in December year 2002, shortly after the fraud was discovered. He was charged with 15 counts of wire, mail and computer fraud—with each count carrying a maximum of five years in prison.

Requirements

1. Describe the symptoms of fraud that might be evident to a fellow Microsoft employee.

   Go to the lecture that covers symptoms if fraud – there are six (lecture 10).

   Accounting Anomalies: Not really there.

   Internal Control Weakness: Ordered his staff to order goods which he then approved.

   Analytical Anomalies: not really there.

   Extravagant Lifestyle – clearly living the high life given the number of cars he had.

   Unusual Behaviour – surely $9m is more software than is needed? Employees should have twigged to the fact that if he needed it he should order and get his supervisor to agree.

   Tips & Complaints: I wonder why the FBI were watching him… no formal program in place.

2. In 2003, Microsoft began putting more emphasis on controlling costs. With the slowing of overall technology spending, executives had ordered managers to closely monitor expenses and gave vice presidents greater responsibility for balance sheets. What positive or negative consequences might this pose to Microsoft in future fraud prevention?

Benefits: Greater scrutiny at a high level. Sets a strong and cultural 'tone from the top'.

Negatives: More sophisticated fraud required to circumvent controls. Puts more power in the hands of the VPs, who might go on to defraud.

3. From the scenario, what are some of the methods Microsoft uses to prevent future frauds?

   Consider the four mechanisms of the previous article – background checks, external audit, internal audit, and anonymous reporting.

   Background checks would be somewhat helpful but wouldn't catch a first-timer. External audit may have found the irregularities, but that process is not designed to catch fraud and would take a while anyway (might never audit the area given MSFT's size). Internal audit would be a good possibility with automatic monitoring of expenditure claims. Anonymous reporting would be most beneficial, likely, given that he needed enforced collusion.

   Strengthening internal controls will give good results – e.g. budget monitoring and exceptions reporting to higher-level management and scrutinisation of expenditure at a higher level.

   If hadn't been so greedy, probably wouldn't have been found out so easily.

5. Case 2 – Cash Sales

Background

Mr Mike H is the cash receipts clerk of DIY Pty Ltd, a large private company which has a chain of 10 hardware stores in a number of locations in Sydney. Mike is responsible for controlling and accounting for all cash receipts through the 10 stores and arranging for the banking of cash received.

You have been requested to provide advice to DIY on its internal controls and fraud risks. Your assistant has completed an internal control review of the cash receipts system and she has given you a copy of the narrative describing the system below:

Description of the System

Mike spends most of his afternoons travelling from store to store. He keeps all cash receipts records on the back seat of his company car. A general review of this documentation revealed that there are many mis-filed and missing documents. Mike does not have sufficient time to keep everything in sequential order.

At each store, Mike collects the cash taken for the day by the cash registers. Each store collects in excess of $20,000 per day. The store managers count the cash taken in advance of Mike’s arrival. Each register produces a record of the day’s transactions and in most cases this is attached to the bag containing the cash. Some managers do not keep this listing, especially when it does not agree to the cash in the register.

When Mike arrives, he checks the difference between the cash counted and the transaction listing. If the difference is less than $1,000, he accepts it as he believes this to be a reasonable variation given the volume of transactions handled. In four of the stores, differences are regularly between $500 and $900. He does not follow up missing transaction listings.

Mike does not recount the cash at each store and no signed representation is taken from each manager as to the accuracy of the count. Mike arrives at the last store just before closing time. He has just enough time to collect the cash and get home in time for dinner. The cash from the 10 stores is left overnight in a safe in Mike’s house. Each morning, Mike goes to head office where he writes up a cash receipts book which summarises his hand-written notes of the previous day’s cash collections. The cash receipts book reports receipts by store.

He then throws away his notes.

He fills out a bank deposit and prepares and posts a single journal entry as follows:

DR Cash
CR Cash Sales

He banks the cash at the local bank branch by 11.00 am. Mike receives monthly bank statements but has asked his secretary to file them immediately as he does not have time to prepare bank reconciliations.

At times when Mike needs some stationery on his rounds, he uses some of the cash to purchase the required items. Because the amounts involved are small, he does not bother completing petty cash vouchers (as required by company policy).

Mike’s supervisor, Ms Mary N, the financial controller, leaves the cash control function to Mike who she believes works well independently. She checks on a monthly basis that the journal entry for cash sales has been processed regularly.

Required

1. What inherent risks exist in this cash receipts system?

   Inherent risks? Well, it’s lousy! It seems everyone knows what’s being done.

Records are incomplete and do not reconcile.

- *Could easily steal cash from managers – should be reconciled by a different person and record as it is handed over kept.*
- *Notes aren't kept!*

No followups to variations.
Reconciliations aren't done
Managers could steal cash – wouldn't be known. Mike could steal cash – wouldn't be known, could easily explain it as variations at the stores.
Supervisor deserves to be shot! Deserves everything she gets when he rips the company off.

2. What is your assessment of the internal controls?

   Completely unreliable. Need to account on a cash basis. Substantive testing would be recommended together with actions required to address internal control weaknesses.

3. What frauds or errors could occur because of control weaknesses?

   Managers and staff could steal cash.

   Mike could commit fraud and modify records, such as they are. Records are so sloppy it would never be found.

   Why $200K in cash in the back of your car? Please!

   Could pretend that he was mugged and take off with the cash. Or could bank the money into his own bank account for a month and it would probably not be noted given the lack of bank recs. Then could skip town ☺.

   What about errors???

4. What internal controls would you recommend?

   Have stores bank their own money and send counter-signed cash register receipts to head office together with deposit slips. Daily deposits recorded and reconciled back to cash register totals. Counter-sign the float by the sales clerk.

   May need to put in a safe over night – although can use night deposit boxes and deposit at the end of the day.

   Daily cashbook balances and bank reconciliations done at head office. Rotated duty and counter-signed by supervisor.

   Variations investigated and noted for reasons why, particularly persistent variations. 5% variation is too high a variation amount. Should not be anywhere near this kind of variation.

   Record bank deposits by store in the journal to reflect in the accounts what occurs at the bank level.