How Organisations Fight Fraud

1. **Fraud Prevention:** this is the most cost-effective way to reduce fraud. Involves two fundamental activities:
    - Create and maintain a culture of honesty and high ethics
        1. Have top management model appropriate behaviour. (if they model bad behaviour then fraud will be more likely to occur)
            Set a proper example/model.
        2. Hire the right kind of employees (through police checks, tests for honesty, references, background investigations…)
        3. Communicate expectations and require periodic written acceptance to the expectations (code of conduct gets rid of any misunderstandings – either cultural…)
            a. Identify and codify appropriate values and ethics
            b. Training employees in fraud awareness (because they will be able to notice it before managers)
            c. Communicating consistent expectations about punishment of violators
        4. Create a positive work environment – frauds are less likely to occur when:
            a. Positive feelings about the organisations
            b. Sense of ownership in the organisation
        5. Enforce policies for handling fraud. Ensure that:
            a. Facts are investigated thoroughly
            b. Firm and consistent actions are taken against perpetrators
            c. Risks and controls are assessed and improved
            d. Communication and training are ongoing

    - Assess the risks for fraud, develop concrete responses to mitigate the risks, and eliminate the opportunities for fraud
        - Organisations should:
            - Identify sources and measure fraud risks
            - Implement preventative and detective controls
            - Create widespread monitoring by employees
            - Have internal and external auditors.

2. **Early Fraud Detection:** 3 primary ways to detect fraud
    a. By chance
    b. By providing "whistle-blowing" systems
        - Must be external system that allows others to call in or submit an anonymous tip of a fraud suspicion.
    c. Data mining
        - Mining for databases for suspicious trends, numbers and anomalies.
3. **Fraud Investigation:**
    - Considerations before investigating fraud:
        - Need management's approval.
        - Pursued only when predication exists

- Predication refers to the circumstances, taken as a whole, that would lead a reasonable, prudent professional to believe a fraud has occurred, is occurring, or will occur (eg reasonable suspicion).
- Investigators rely heavily on interviews, computer searches, and accounting records and internal controls.

- 4 types of evidence in fraud investigations:
  - **a.** Testimonial Evidence:
    - Evidence gathered from individuals by interviewing, interrogation and honesty tests.
  - **b.** Documentary Evidence:
    - Gathered from paper, computer, or other sources.
    - Techniques include:
      - Document examination, data mining, public record searches, audits, computer searches, net worth calculations, financial statement analysis, corporate databases & email servers.
  - **c.** Physical Evidence:
    - Need other forensic analysis by experts. Use such things as fingerprints, tire marks, weapons, stolen property, identification numbers, marks on stolen objects and other tangible evidence.
  - **d.** Personal Observation:
    - Evidence that is sensed (seen, heard, felt…) by the investigators.
      - Techniques include:
        - Invigilation: when you control all transactions within the company. Can help determine materiality. Compare a period free from fraud.
        - Surveillance
        - Covert operations
- The Fraud Element Triangle:
  - Theft Act: catch perpetrators in the embezzlement act or to gather information about the actual theft acts.
  - Concealment**:** focus on records, documents, computer programs and servers, and other place where perpetrators conceal their dishonest acts.
  - Conversion: Search for ways the perpetrators spent/used their stolen assets.
- **Steps to conduct a fraud investigation:**
  1. Undertake only to "establish the truth"
  2. Experienced and objective investigators
  3. Confidentiality. Don't share information about investigations as they can jeopardise them.
  4. Only work out what you need to know – establish the facts.
  5. Evidence independently corroborated
  6. No questionable investigation techniques
  7. Fair and objective communication

4. **Follow-up Legal Action and/or Resolution:**
   - **a.** No Legal Action:
     - What are the consequences of taking no action? (eg cost of action vs inaction).
   - **b.** Civil Case:
     - To recover money or assets taken
     - Quite rare with employee fraud as most of the money has been spent on vices.

- More common when other organisations are involved.
- May sue the auditors (if they should have seen it) or others with 'deep pockets'

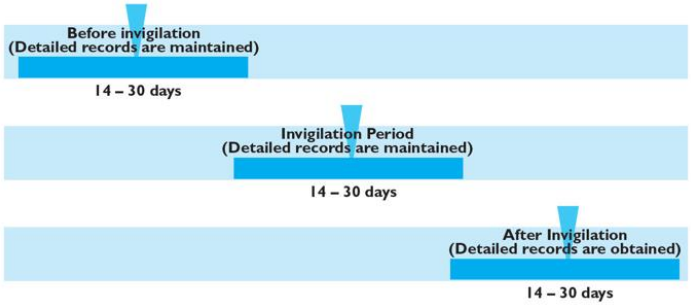
c. Criminal Case:

- Only be brought by law enforcement agencies.
- Usually involves fines and/or imprisonment
- More difficult to get a criminal conviction than a judgement in a civil case

d. Both b & c:

Invigilation

Business is taken over by forensic accountant so that you can observe a period of non-fraud. There are strict temporary controls implemented. Also allows for the close supervision of suspects. Invigilation occurs over at least 3 months:



Each period needs to occur over 2 weeks to a month.

First period is invigilation free so that you get detailed records of when fraud is occurring.

Next period is invigilation so you can see detailed records of when no fraud is occurring.

Final period is after invigilation, here we see a period with fraud again and can compare and find where fraud is occurring.

Physical Evidence

Involves analysing objects such as:

- Inventory, assets, and broken locks
- Substances such as grease and fluids
- Traces such as paints and stains
- Impressions such as cutting marks, tire tracks and fingerprints
- Computer searching

Electronic Evidence

(gathering electronic evidence is highly technical. Can need computer forensics specialists)

Step 1: Secure the device and perform initial tasks.

- Need to have the legal right to seize the hardware
- Exercise care with respect to chain of custody, evidence marking…
- Take pictures (firm camera not own) of the seizure site and have neutral (impartial, 3rd party) witnesses at the scene.
- Turn off computer by cutting the power to the machine not normally.

Step 2: Clone the device and calculate a CRC checksum

- Perform a bit-for-bit copy of the entire hard drive
- Calculate the CRC checksum
    - Cyclic redundancy check (CRC) number: a calculation based on the contents of disk/file. Any change to disk/file will change the CRC checksum.
- Seal away the original disk
- Perform investigation on the cloned copy

Step 3: Search the device manually

Common areas to search include:

- Computer logs such as Web activity, recent files on the Start menu, Web favourites, browser history…
- The Documents folder – most applications save data to this location. Also check related folders.

- Trash can/Recycle bin
- USB drives, CDs, or other media found around the computer
- Recently loaded files listed in the File menu of many applications
- Chat logs and email client caches

Step 4: Search the device using automated procedures

Forensic Software Packages

- Guidance Software's Encase Forensic Edition
- AccessData's The Forensic Toolkit

Open Source Packages

- E-fense Inc.'s Helix
- Backtrack-linux's Backtrack

WEEK 9

REVENUE AND INVENTORY RELATED FINANCIAL STATEMENT FRAUDS

Revenue-Related Fraud

- The most common accounts manipulated when perpetrating financial statement fraud are revenues and/or receivables (in financial statement fraud). 2 reasons for the prevalence of revenue-related financial statement fraud:
  - The availability of acceptable alternatives for recognising revenue (when earnt, when received, when stock sold) (also problems with returns being recognised…)
  - The ease of manipulating net income using revenue & receivable accounts
- Over half of all financial statement frauds involved revenues and/or accounts receivable accounts, according to COSO-sponsored research

Revenue related fraud exposures should be considered in every business.

Common revenue-related fraud schemes are:

- Related-party transactions: in consolidated reports (like Enron where related party revenues were recognised but all costs and liabilities were deferred)
- Sham sales: (relates to when revenues are recognised like OneTel where 48 months of revenues were accounted for when customers signed up for plan even though some of these customers would pay amounts owed)
- Bill-and-hold sales
- Side agreements
- Consignment sales
- Channel stuffing
- Lapping or kiting
- Redating or refreshing transactions: (can be photoshopped, backdated, redated, appear like they happen many times)
- Liberal return policies
- Partial shipment schemes
- Improper cutoff
- Round-tripping

Sale process allows for fraud at every step:

Identify Revenue-Related Fraud Symptoms

- Fraud is rarely observed (revenue-related fraud are incredibly hard to find)
- Fraud symptoms can be divided into 6 categories:
  - Analytical symptoms (strange relations b/w accounts…)
    - Revenue/sales that appear to high
    - Sales discounts that appear to low
    - Sales returns that appear too low
    - Bad debt expense that appear to low
    - Accounts receivable that appear too high or are increasing too fast
    - The allowance for doubtful debts appears too low
    - Too little cash is collected relative to reported revenues
  - Accounting/documentary symptoms (problems w/ accounting systems)
    - Unsupported or unauthorised revenue-related balances or transactions
    - Missing documents in revenue cycle
    - Photocopies where original should exist
    - Significant unexplained items on bank and other reconciliations
    - Revenue-related ledgers (sales, cash receipts…) that do not balance.
  - Lifestyle symptoms (fraudsters lifestyle becoming extravagant)
    - Major sales of company stock around earning releases or other unusual dates
    - Significant bonuses tied to meeting earnings forecasts.
    - Executives' personal net worth tied up in company stock.
  - Control symptoms (internal control missing)
    - Management overriding (as management are the normally the ones who commit financial statement fraud) significant internal control activities related to revenue cycle (BEST WAY TO FIND IS IN MINUTES FOR BOARD MEETINGS)
    - New, unusual or large customers that appear not to have gone through the customer approval process.
    - Weaknesses in the cut-off processes or other key accounting processes.
  - Behavioural and verbal symptoms

- Inconsistent, vague or implausible responses from MGMT or employees arising from revenue inquiries or analytical procedures (from forensic accountant).
- Forensic accountant denied access to facilities, employees, records, customers, vendors or others from whom revenue-related audit evidence might be sought.
- Undue time pressures imposed by management to resolve contentious or complex revenue related issues.

- Tips & complaints
  - Tips or complaints that revenue-related fraud might be occurring, either from the company whistleblower system or in other ways
  - Revenue frauds disclosed at companies with which this company does significant business

Inventory or COGS Frauds:

If inventory is overstated then:

- For example, when examining an Income Statement, if inventory is overstated, then:

Income Statement Account	Outcome
Gross sales/revenue	Not affected
Sales returns	Not affected
Sales discounts	Not affected
= Net revenues/sales	Not affected
– Cost of goods sold (COGS)	Understated
= Gross margin	Overstated
– Expenses	Not affected
= Net income	Overstated

This has an effect on the next period:

COGS calculation	Period 1 (Overstatement of ending inventory)	Period 2
Beginning inventory	Not affected	Overstated
Plus: Inventory purchases	Not affected	Not affected
Less: Vendor inventory returns	Not affected	Not affected
Less: Inventory purchase discounts	Not affected	Not affected
= Goods available for sale	Not affected	Overstated
Less: Ending inventory	Overstated	Not affected
= COGS	Understated	Overstated