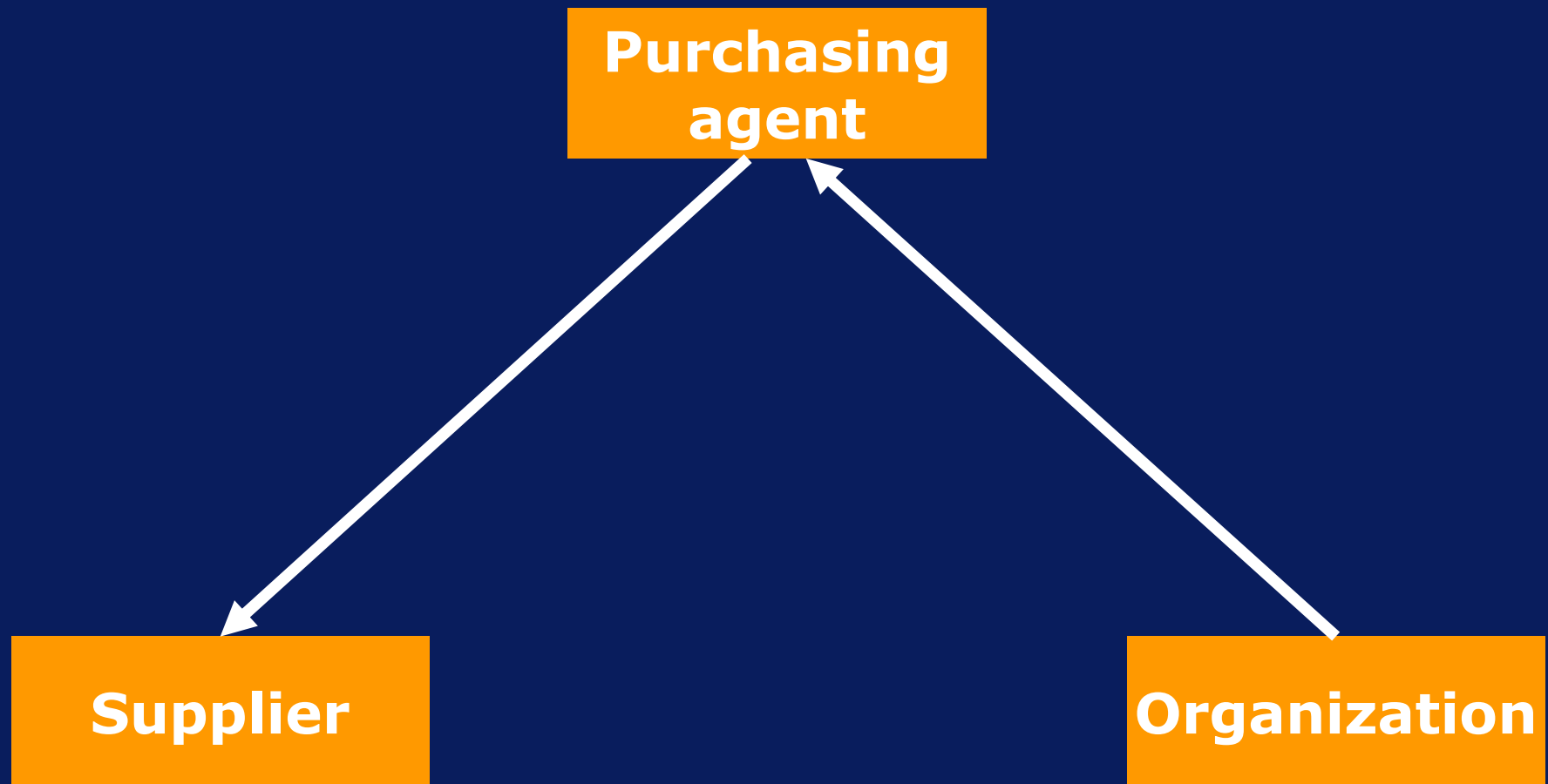


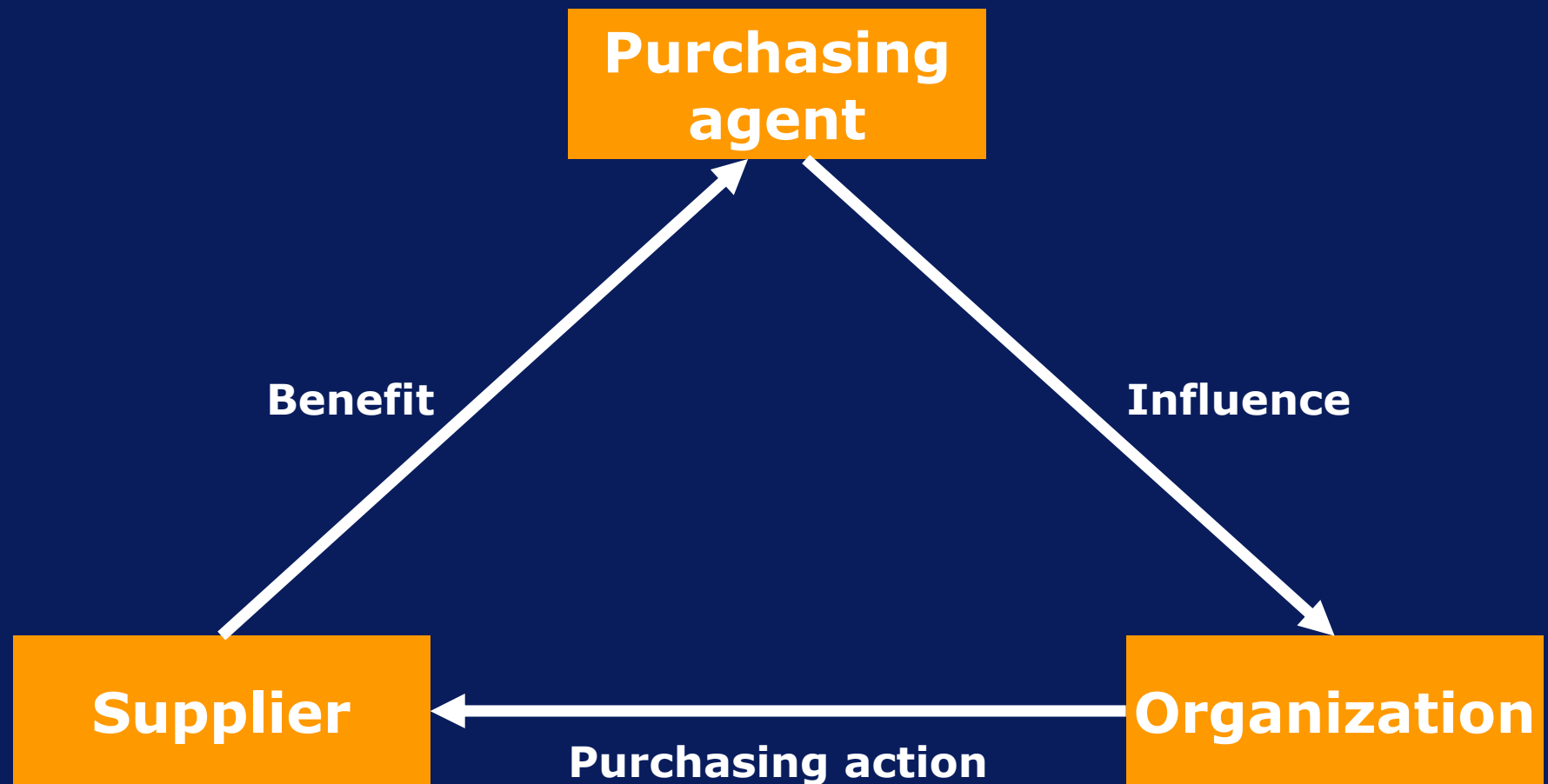
# Kickbacks and corruption (1)



# Kickbacks and corruption (2)



# Kickbacks and corruption (3)



# Bid rigging

## • What happens?

- Employee rigs tender to ensure corrupt supplier wins
- Corrupt supplier often not most economical, paid more quickly, offers no discounts
- Contract is worded loosely to allow for “extras”, “variations”, “change orders” over and above the fixed price
- Corrupt supplier almost always gets the kickback back through:
  - Higher prices
  - inferior quality (bait and switch)

# Corruption and kickbacks: bid rigging

## Red flags:

- Specifications designed to only fit 1 contractor
- Advance release of specifications to 1 contractor
- Unnecessary sole source justifications, usually stated to be for “technical” superiority of chosen vendor (especially IT!)
- Exclusion of qualified contractors from bid process
- Splitting requirements into phases
- Vague specifications
- Limited time to submit bids
- Sharing legitimate bidder information with favoured vendor
- Inadequate search/shortlisting of qualified vendors

# Corruption and kickbacks: bid rigging

## Red flags (continued):

- Employee ownership interest in favoured vendor
- Acceptance of late bids
- Changes made in vendor bid documents (especially if submitted electronically)
- Improper disqualification of bids
- Acceptance of non responsive bids
- Unnecessary contacts with preferred vendor
- Inappropriate evaluation criteria/scoring(watch for pattern)
- Inappropriate weight between technical and financial criteria
- Changes to contract shortly after award

# The case of the phantom supplier

## Office Supplies Limited

P.O. Box 101  
Toronto, Ontario  
M7G 8J9  
(416) 975-3462

**AS26374L**

January 31, 1995

Sold to:

Large Municipality  
200 Eglinton Ave. East  
Toronto, Ontario  
M8G 3E4

Quantity	Description	Unit price	Amount
1 dozen	drafting pads	14.95	179.40
		tax	14.36
			<b>\$193.76</b>

# Office supplies limited – red flags

- no salesmen visits
- no product catalogue
- no Christmas card
- telephone number was for an autobody shop
- invoices always under \$500
- cheques always under \$2,000
- all invoices approved for payment by Mr. Jones
- Mr. Smith also responsible for accounts payable

# Expense account padding

# Topics covered

- Expense policy
- Typical expense account fraud
- Why they do it/rationalizations
- What about when your employees are inappropriately entertained on someone else's expense account?

# Star-Ledger

New Jersey

April 4, 2006

“The harshly critical findings, in a report released yesterday by the federal monitor overseeing the university, also found a top administrator systematically abused his expense account, including the freewheeling use of hotel rooms after “late-night meetings” that never occurred, and the rental of an Alfa Romeo for a business trip.”

# Scandal shakes public radio

March 17, 2006

Men kept freebies meant for station, prosecutors allege

The sedate, urbane world of public broadcasting was rattled Thursday as prosecutors charged three former employees of Michigan Public Media with illegally accepting golf club memberships, Persian rugs, airline tickets and massages in exchange for on-air considerations at the state's top public radio station

# Expense policy

- Travel and hospitality
- Business purpose for hospitality
- Reasonable in amount
- Substantiated by receipts and other information
- General versus specific guidelines:
  - Minibars
  - In room movies
  - Mileage/auto costs
  - Meals/per diems
  - Cell phones/blackberries
- Approval process
  - Chief Executive
  - others

# Typical expense account fraud

- No real business purpose
- Double dipping
- Changing amounts
- Outright fraud

# Why they do it/rationalizations

- Immaterial
- Sense of entitlement
- I would make more in the private sector
- I get my secretary to do my expense report, therefore it's her fault!
- I work 24/7

# What about when your employees are inappropriately entertained on someone else's expense account?

- Policy on keeping a log of entertainment/reporting events
- Accepting inappropriate entertainment
- Wonder how the supplier gets reimbursed? Bill cost through to client
- Courts will respect company policy to take dishonesty seriously if company consistently enforces policy

# What to do when fraud is suspected

- Meet with counsel, other specialists and senior company official to discuss the allegation
- Develop an investigative and legal strategy regarding the allegation
- Commence execution of the strategy
- Identify internal and external resources to assist the investigation
- Meet frequently to evaluate findings and re-evaluate strategy

# What not to do when fraud is suspected

- Ignore your suspicions
- Accuse the suspect
- Discuss the issue with the suspect
- Openly gather information from others that may alert the suspect
- Solely use internal resources to investigate allegations against senior officers
- Boot up the suspect's computer

# Day 1 do's

- Limit the number of people who 'need to know'
- Assess the situation and all available information
- Consider risk/exposures
- Develop an investigative strategy
- Document, document, document

# Day 1 don'ts

- React in a “Knee-Jerk” fashion
- Confront the suspect
- “Rummage” for evidence (electronic and paper)
- Over-react

# Investigation plan

- Who is in charge?
- Investigation steps
- Investigation tools
- Who does what?
- What is the budget?
- Communication
- Press
- Dealing with the suspect

# To investigate or not, that is the question

- Investigate
  - The extent and magnitude
  - Set an example
  - Company policy/ethics
  - Recover losses
    - Civil
    - Insurance
  - Terminate wrongdoers
  - Defend dismissal action
- Don't investigate
  - Cost
  - Amount of loss small
  - No insurance
  - Adverse publicity
  - Don't want to know
  - Too close to the top

# Evidence

- Documentary
- Statements by suspect
- Eye witnesses (testimonial)
- Physical
- Expert
- Circumstantial
- Electronic evidence
  - Email
  - Drafts

# Obtaining evidence – Criminal

- Court orders
  - Search warrant
  - General warrant
  - Must include assistance order for civilians
- Plain view doctrine
- MLAT/Letter of request

# Obtaining evidence – civil

- Involuntary access
  - Anton Pillar Order
    - Affidavit process
- Voluntary access to client's facility
  - Surreptitious searches (office/desk/computer)
  - Limits

# Interviewing suspects and witnesses



# The electronic “Haystack”

- Nearly all information is created electronically
- Millions of transactions of legal relevance are
  - being conducted electronically
- Only 30% of all information makes it to paper
- It is estimated that 6.9 trillion e-mail
  - messages were sent in 2000(Atlanta Business Chronicle)

# What is computer forensics

- Computer forensics is the identification, collection, preservation, analysis and presentation of relevant electronic data in a manner that will allow it to be admissible in a legal proceeding

# What can be found

- E-mail (Microsoft Exchange, Microsoft Outlook, web based etc.)
- Hidden, password protected, encrypted documents and files
- Files that have been printed from the system (Enhanced Meta Files)
- Databases, proprietary software, “all” user input
- Recent files opened, accessed, created etc.
- Online activity – including secure banking
- Basically, all user input

# Why use computer forensics

- Time is of the essence (Intellectual Property)
  - Identify and obtain all relevant facts
  - Corroborate sources of information
  - Assist counsel in discovery process
  - Expert interpretation of electronic data recovered
  - Substantiate or refute allegations
  - Difference between guessing and knowing what occurred with a degree of certainty
  - Best evidence

# Computer evidence

- Interview of subjects
- Identify potential evidence sources
  - Off-site file storage – paper and electronic
  - Locations of computer systems and users – principal offices, remote users, home computers
  - Other storage mediums – PDA's, electronic storage media – eg: ZIP™, JAZ™, Disk on Key™ archived tape storage, etc.
  - Execution of Anton Pillar order(s) (Civil Search Warrant)
- Acquisition of electronic evidence from computer systems

# Collection of evidence

- Maintaining strict forensic practices at site
  - Not activating any power devices – light switches etc.
  - Photographing and marking of target computers
  - Documentation of site including other materials, manuals, books, software
  - Inspecting surrounding area for passwords, www sites
  - Labeling and marking of any material seized
- Continuity of exhibits
  - What, where, when, why and who – possession of exhibits
  - Chain of custody, continuity, integrity – sealed, locked etc.
  - Best Evidence rule

# Timely collection of evidence

- Computer hard drives are constantly being written to when systems in use
- Files, which may afford evidence can be overwritten by other material
- Hard drives can fail or become corrupted
- Computers, and hard drives, especially laptop can go “missing”
- Sooner information is gathered – better to associate to user – not someone else who inherited the computer

# Computer forensics finds the “Smoking Chip”

- Case #1
  - Retained by a law firm to conduct an independent review of financial records
  - Concern about overstatement of 611 million Yen over several years
  - Conducted independent review technology company’s financial records found:
    - Attempt to conceal 1,600 of CEO’s files
    - \$8 million (US) in fictitious sales contracts and receivables
    - Evidence of kickbacks worth >\$100,000 U.S.
    - Record of a drafted confession letter

# Computer forensics finds the “Smoking Chip”

- Case #2

- Retained by an organization to conduct an investigation into a suspected kickback scheme involving the organization’s purchasing agent
- Concern about purchasing agent steering work to certain suppliers
- Computer forensics found:
  - Invoice from a company set up by the purchasing agent to one of the organization’s suppliers
  - Banking information indicating payments made from the supplier directly to the purchasing agent
  - Email traffic between the supplier and the purchasing agent wherein the supplier offered to give the purchasing agent a one third interest in his business
  - The above information had been “deleted” by the purchasing agent (or so he thought!)

# Practical considerations

- Cost benefit analysis
- Fishing expeditions are expensive
- Covert vs. overt
- How many computers did the suspect have access to?

# Control environment

- Tone at the top
  - Management involvement and accountability for antifraud activities
  - assessments of the tone through anonymous cultural surveys, inquiries and interviews
  - internal audit review
- Effective audit committee and board oversight
- Effective involvement from internal audit
- Ethics/whistleblower hotlines
- Training
- Code of conduct/ethics
  - provisions related to conflicts of interest
  - related party transactions, illegal acts, and fraud; confirmations
- Hiring and promotion standards and procedures
- Responses to control deficiencies and allegations of fraud

# Antifraud control activities

- Link or map identified fraud risks to control activities
- Evaluate the effectiveness of existing controls and implement additional control activities where necessary
- Implementation of preventative and detective controls
- Controls to restrain misappropriation of assets that could result in a material misstatement of the financial statements
- Address the risk of management override of controls (journal entries, bias of estimates, non-routine or unusual transactions)

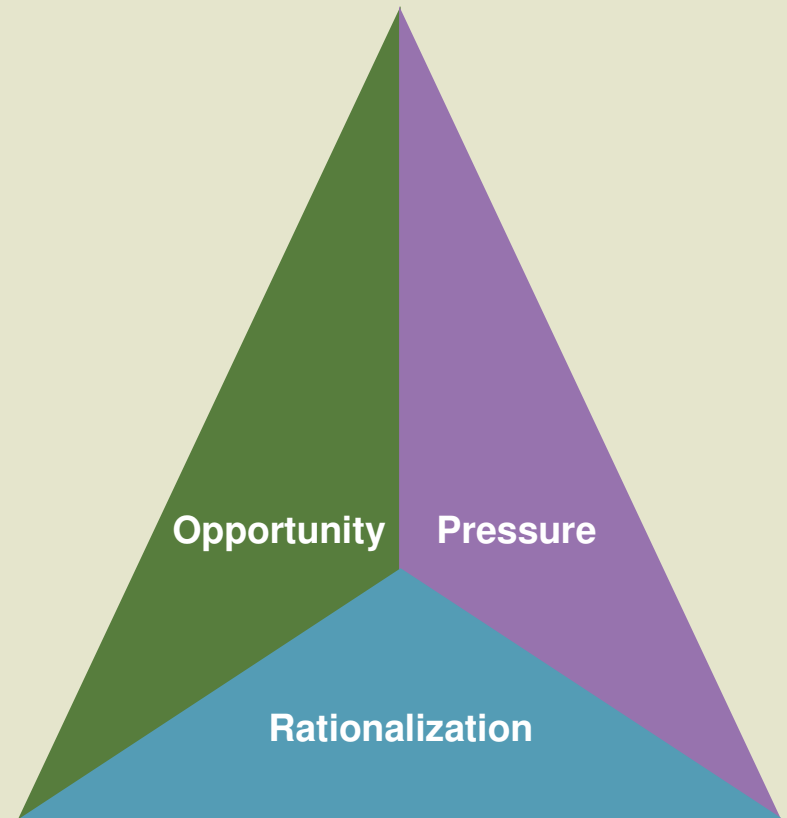
# Information & communication

- Effective communication of antifraud programs and controls and management's commitment to ethics
- Training
  - Code of ethics
  - Fraud prevention
- Knowledge management
  - collecting and sharing information regarding fraud risks, control activities and remediation
- Information systems & technology
  - Consideration of IT fraud risks, security and access controls
  - Utilize IT to prevent and detect fraud
  - Investigate computer misuse

# Monitoring

- Assessment of the effectiveness of existing antifraud controls
- Monitoring by management
  - evaluation of design and effectiveness of control activities
- Internal audit activity and evaluations
  - appropriate level of activity based on size and complexity of organization, address fraud risks in annual audit cycle
- Effective audit committee oversight

## Fraud triangle



Source: Donald D. Cressey, "Other People's Money: A Study in the Social Psychology of Embezzlement"

# Step one: evaluate fraud risk factors

- Events or conditions that indicate incentives/ pressures to perpetrate fraud, opportunities to carry out the fraud, or attitudes/rationalizations to justify a fraudulent action
- Past frauds in the organization and industry
- Evaluate factors at the entity level, significant locations, and significant accounts or business processes
- Involve personnel from various levels of the organization (management, business process owners, internal audit, audit committee)

## Step two: identify possible fraud schemes and scenarios

- Involvement of proper personnel
  - Management, business process owners, internal audit
- Brainstorm possible fraud schemes and scenarios
- Consider frauds at organization and industry
- Identify possible fraud schemes – without consideration of the existence or effectiveness of internal controls

# Step three: prioritize identified fraud risks

- Evaluate possible fraud schemes:
  - *Type*
  - *Likelihood*
  - *Significance*
  - *Pervasiveness*
- Additional considerations should be given to those risks considered to be;
  - Likely
  - Significant; and/or
  - Pervasive

## Step four: evaluate whether mitigating controls exist/are effective

- Map or link fraud risks to internal control activities
- Evaluate controls to determine if they sufficiently mitigate the identified fraud risks or if additional emphasis should be placed on existing controls
- Design and implement additional antifraud controls for identified fraud risks where controls are not already present
- Special consideration given to the risk of management's override of controls

# Professional scepticism

- All signing authorities should adopt an attitude of professional skepticism, recognizing that circumstances may exist that causes the documents or representation to be improper
- It means the a signing authority officer should make a critical assessment, with a questioning mind, of the sufficiency and appropriateness of supporting documents being provided and is alert for evidence that contradicts or brings into question the reliability of the documents or employees representations
- Professional skepticism does not mean a signing authority is obsessively sceptical or suspicious

# Professional scepticism (cont'd)

- The attitude of professional scepticism is necessary throughout an approval process in order to reduce the risk of overlooking suspicious circumstances
- In those instances where the transaction data is inconsistent with the source documentation supporting that transaction, the general ledger should be updated to reflect the correct information
- Prior to make such adjustments these errors should be monitored in order to ensure the appropriateness of the adjustments and also be approved by the appropriate level of management

# Public accountability – a sense of belonging

“The absence of commitment to **corporate cultural** standards leads more easily to deviant forms of behaviour by individual employees, who may disregard the reputation of their employer or even their own if a quick profit is to be made.”

**Source:**

Corporate Loyalty: A Trust Betrayed, Copyright Brian A. Grosman, 1988



# Deloitte.

© Deloitte & Touche LLP and affiliated entities.

Deloitte, one of Canada's leading professional services firms, provides audit, tax, consulting, and financial advisory services through more than 6,800 people in 51 offices. Deloitte operates in Québec as Samson Bélair/Deloitte & Touche s.e.n.c.r.l. The firm is dedicated to helping its clients and its people excel. Deloitte is the Canadian member firm of Deloitte Touche Tohmatsu.

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, its member firms, and their respective subsidiaries and affiliates. As a Swiss Verein (association), neither Deloitte Touche Tohmatsu nor any of its member firms has any liability for each other's acts or omissions. Each of the member firms is a separate and independent legal entity operating under the names "Deloitte," "Deloitte & Touche," "Deloitte Touche Tohmatsu," or other related names. Services are provided by the member firms or their subsidiaries or affiliates and not by the Deloitte Touche Tohmatsu Verein.



Member of  
**Deloitte Touche Tohmatsu**