



What is Fraud?

Definition (Fraud)

In a broad stroke definition, fraud is a deliberate misrepresentation which causes another person to suffer damages, usually monetary losses

Many fraud cases involve complicated financial transactions conducted by 'white collar criminals', business professionals with specialized knowledge and criminal intent.

Fraud is not easily proven in a court of law.



Definition

According to the Institute of Internal Auditors (IIA), “The internal auditor should have sufficient knowledge to identify the indicators of fraud but is not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud.” Furthermore, the IIA maintains that “detection of fraud consists of identifying indicators of fraud sufficient to warrant recommending an investigation.”

The IIA’s Practice Advisory 1210.A2 further states, “Internal auditors are responsible for assisting in the deterrence of fraud by examining and evaluating the adequacy and effectiveness of the system of internal control, commensurate with the extent of the potential risk exposure in the various segments of the organization’s operations.”

The auditor's main role is learning to be effective at detecting possible frauds. This is accomplished through training and understanding of the symptoms of fraud for various business processes, designing audit steps with fraud in mind, and following up on tests that reveal weak deterrent controls.



Types of Fraud

Conflict of interest

Bribery

Embezzlement

Forgery

Filing False Claims

Kickbacks Overbilling

Theft

Theft of Time

Unauthorized Use, and abuse

All of these are criminal acts for personal gain, we usually classify them under “FRAUD”.

Detrimental Effects of Fraud

- Loss of confidence by customers, lenders, regulators, stockholders
- Loss of sales, market share, influence
- Loss of access to financing
- Withdrawal or refusal of licenses
- Ejection of management
- Bankruptcy/liquidation



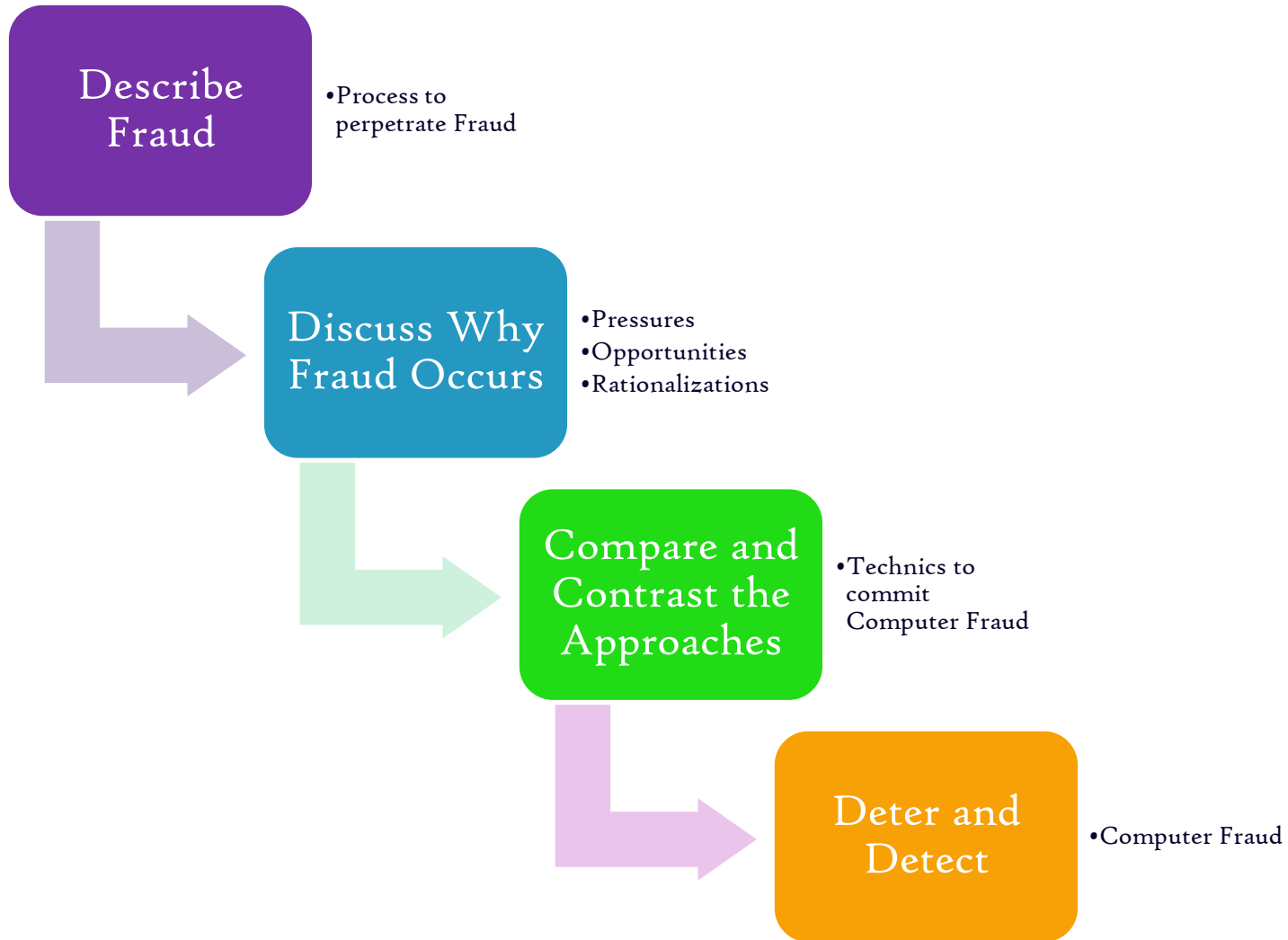
Elements Contributing to Fraud Environment

Corporation:

- * Too much trust in employees
- * Lack of proper procedures for authorization
- * Lack of personal financial information disclosure (for bank frauds)
- * No independent checks on performance
- * Lack of adequate attention to detail
- * Non segregation of duties
- * No separation of accounting duties
- * Lack of clear lines of authority
- * Department infrequently audited/reviewed
- * No conflict of interest statement required
- * Inadequate documents and records.



Learning Objectives



Learning Objective 1

The Fraud Process

Most frauds involve three steps.

The theft of
something

The conversion
to cash

The
concealment

The Fraud Process

What is a common way to hide a theft?

- to charge the stolen item to an expense account

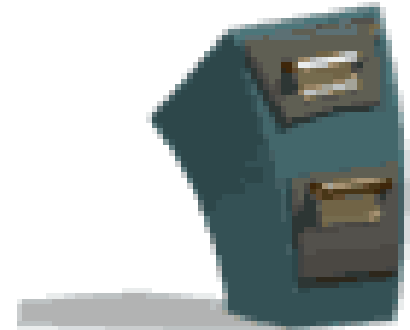
What is a payroll example?

- to add a fictitious name to the company's payroll



The Fraud Process

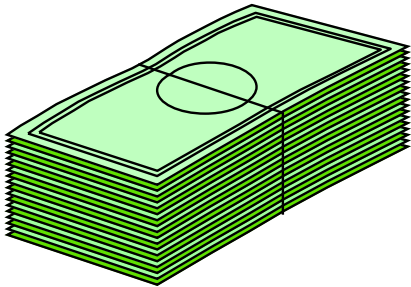
- What is lapping?
- In a lapping scheme, the perpetrator steals cash received from customer A to pay its accounts receivable.
- Funds received at a later date from customer B are used to pay off customer A's balance, etc.



The Fraud Process

What is kiting?

- In a kiting scheme, the perpetrator covers up a theft by creating cash through the transfer of money between banks.
- The perpetrator deposits a check from bank A to bank B and then withdraws the money.

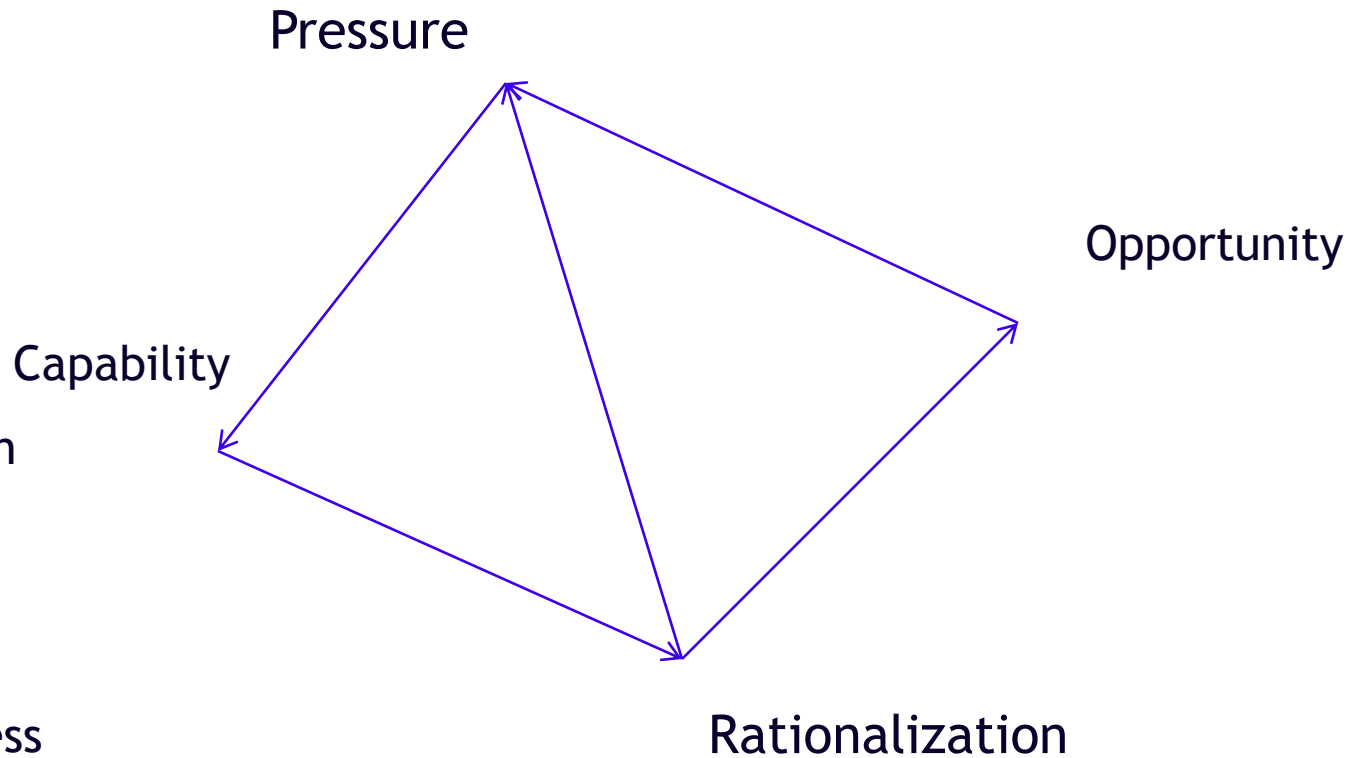


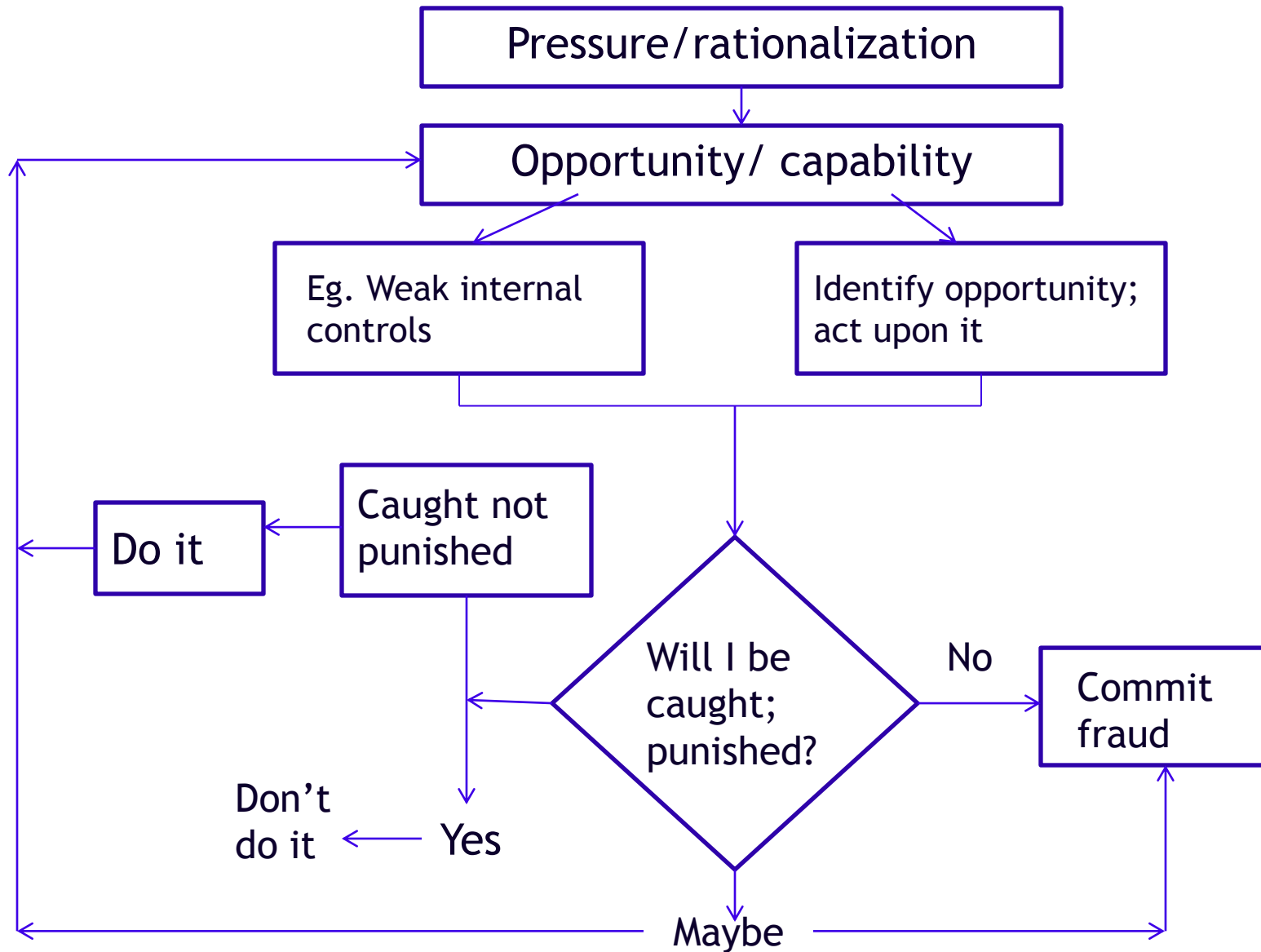
The Fraud Process

- Since there are insufficient funds in bank A to cover the check, the perpetrator deposits a check from bank C to bank A before his check to bank B clears.
- Since bank C also has insufficient funds, money must be deposited to bank C before the check to bank A clears.
- The scheme continues to keep checks from bouncing.



The triangle extended: the fraud diamond - Wolf & Hermanson - 2004





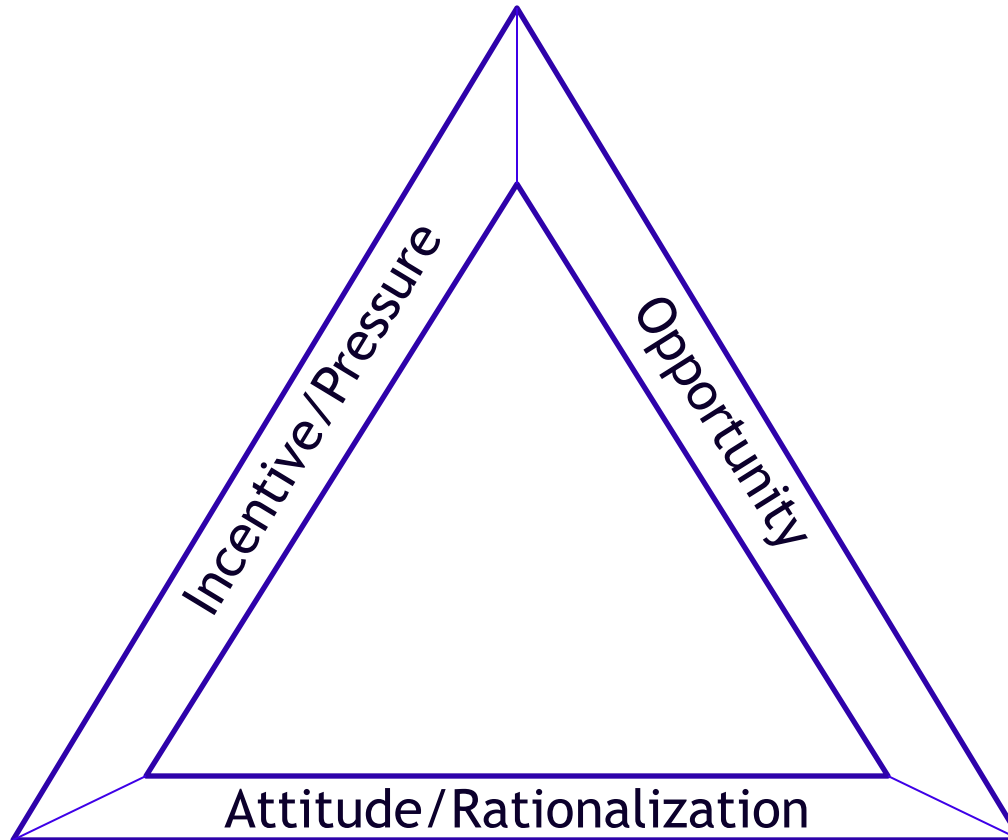
Why Fraud Occurs Contd...

Three conditions are necessary for fraud to occur:

1. A pressure or motive
2. An opportunity
3. A rationalization



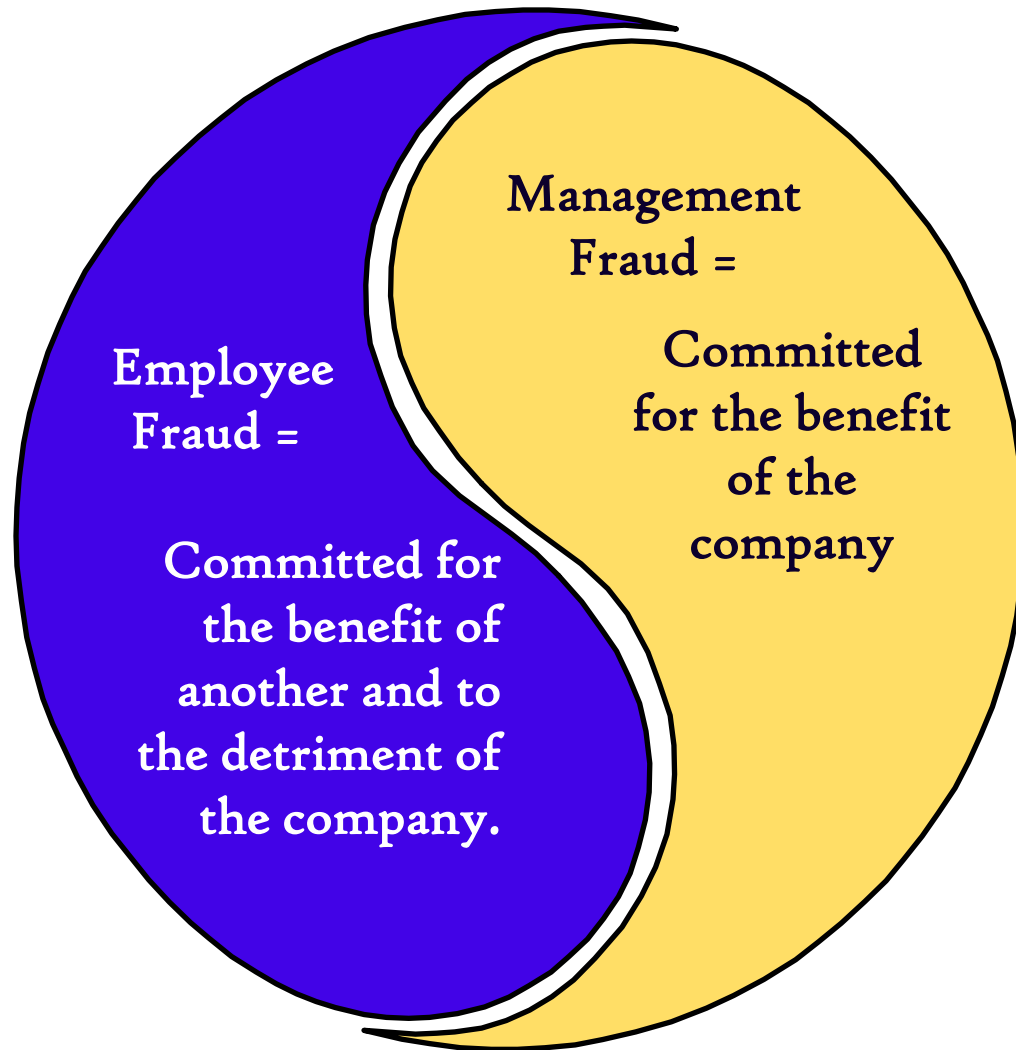
Ronelle's Fraud Triangle



Iceberg Theory of Dishonesty

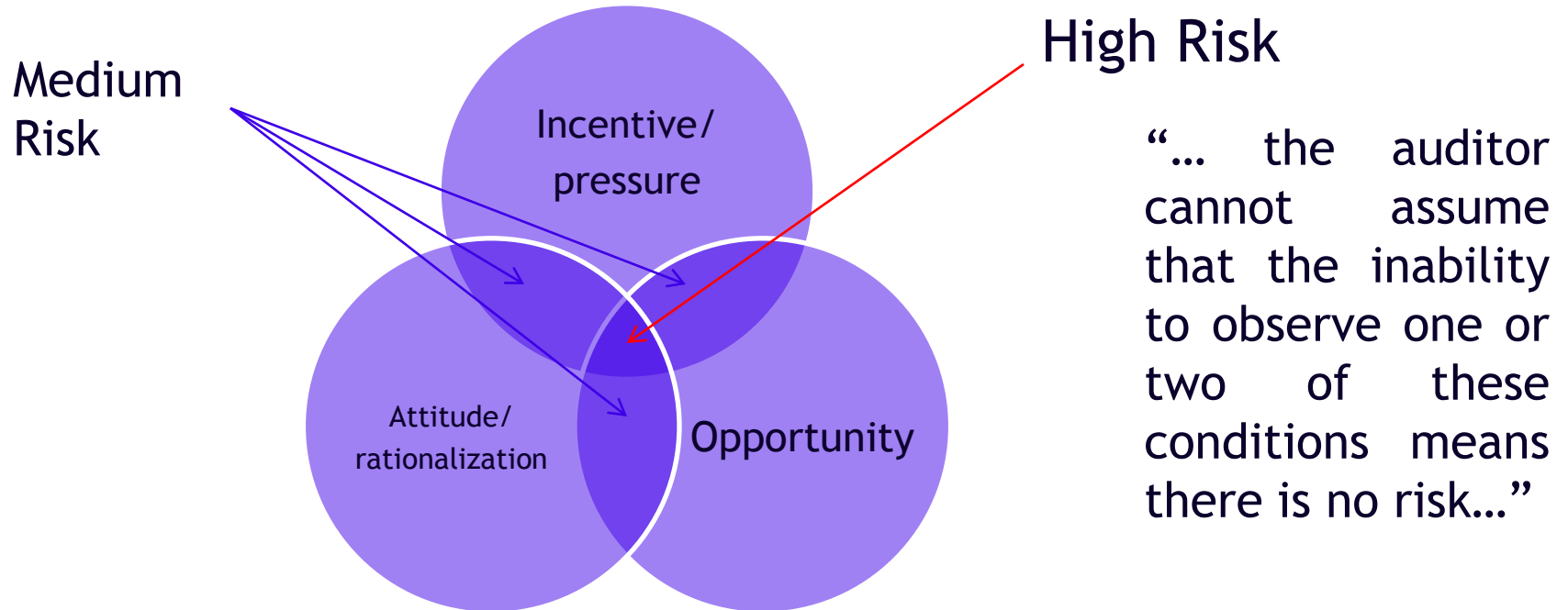


Fraud Risks



Fraud Risk Model

“ The auditor should not assume that all 3 conditions must be observed or evident before concluding that there are identified risks. “



“... the auditor cannot assume that the inability to observe one or two of these conditions means there is no risk...”

Learning Objective 2

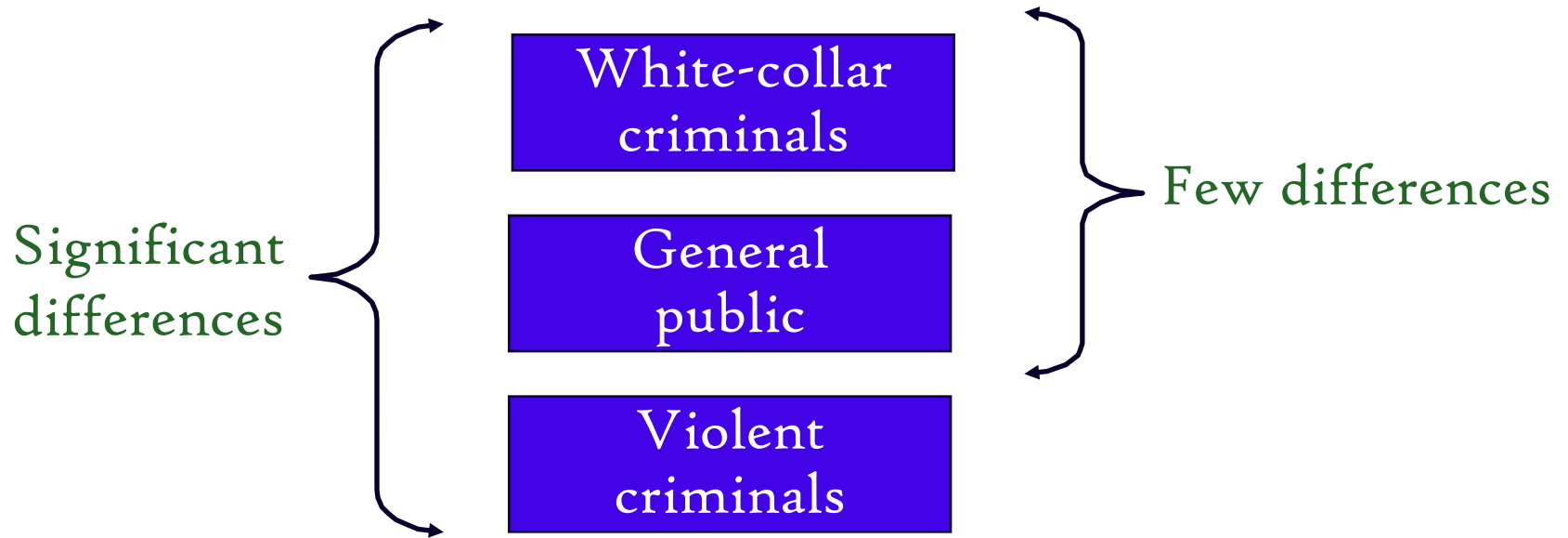
Why Fraud Occurs

Discuss why fraud occurs, including the pressures, opportunities, and rationalizations that are present in most frauds.



Why Fraud Occurs Contd...

Researchers have compared the psychological and demographic characteristics of three groups of people:



Why Fraud Occurs Contd...

What are some common characteristics of fraud perpetrators?

- Most spend their illegal income rather than invest or save it.
- Once they begin the fraud, it is very hard for them to stop.
- They usually begin to rely on the extra income.



Frauds are committed by people we trust.



The Fraud Triangle

(Why good people do the wrong thing)

Pressure (Real or Perceived)

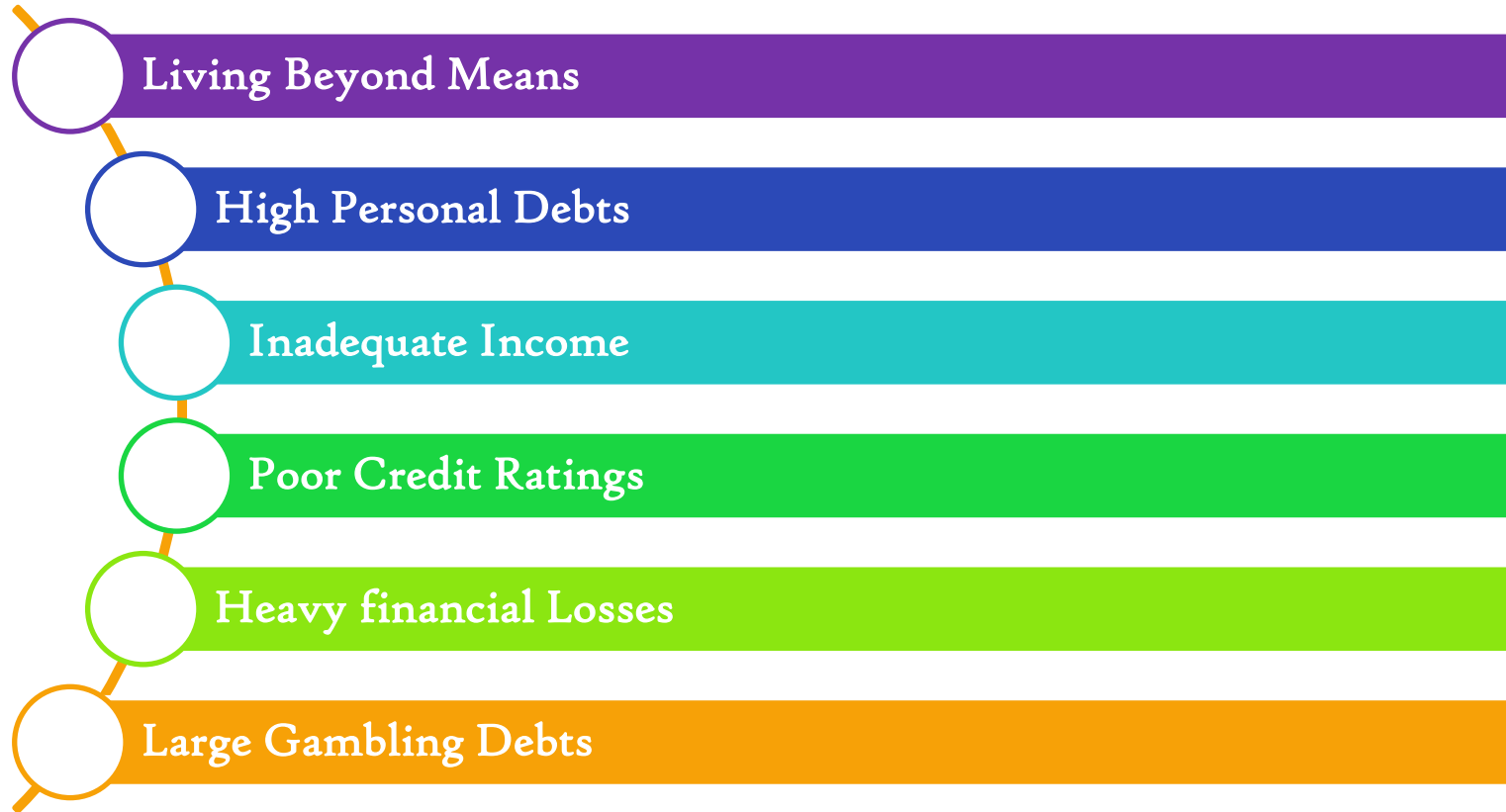


Opportunities, Consequences,
and Likelihood of Detection
(Real or Perceived)

Rationalization

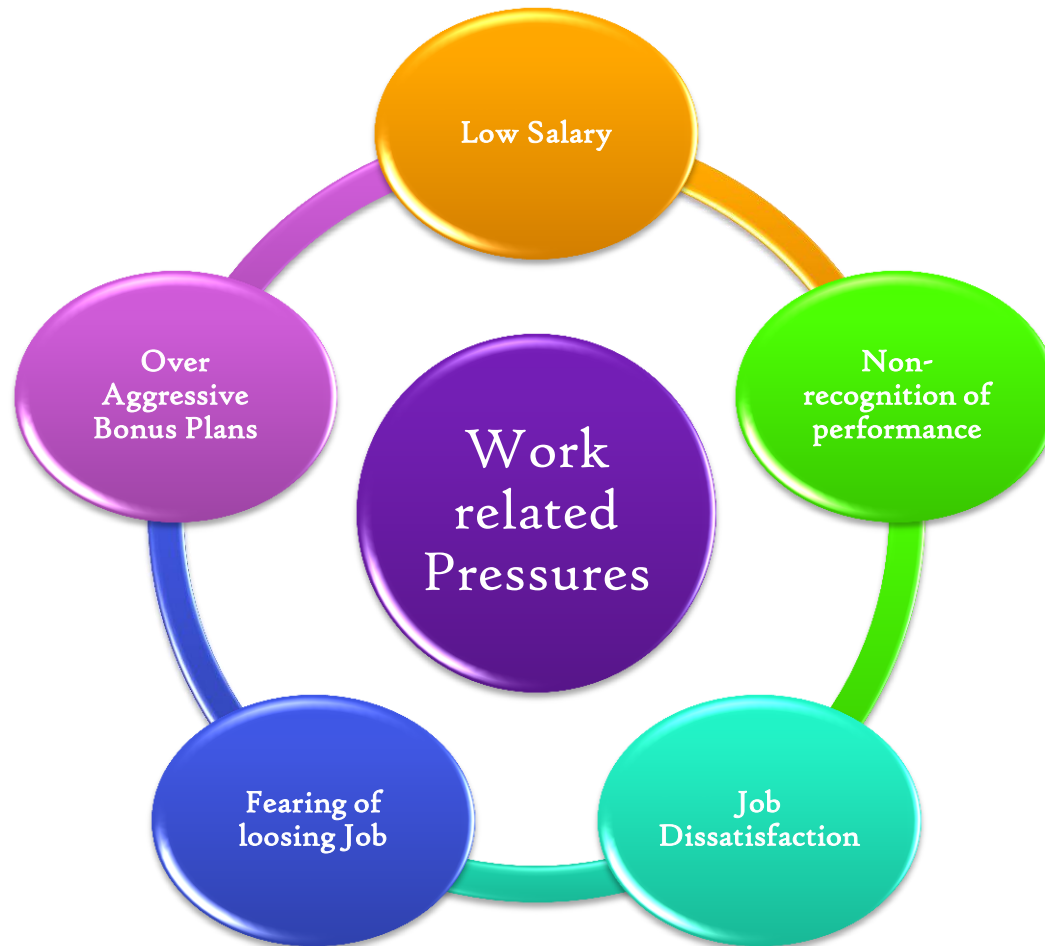
Pressures

What are some *financial* pressures?



Pressures

Work related pressures



Pressures

Other pressures

Challenge

Family/Peer Pressure

Emotional Inability

Need for power to control

Excessive pride and ambitions

Opportunities

- An opportunity is the condition or situation that allows a person to commit and conceal a dishonest act.
- Opportunities often stem from a lack of internal controls.
- However, the most prevalent opportunity for fraud results from a company's failure to *enforce* its system of internal controls.



Rationalizations

Most perpetrators have an excuse or a rationalization that allows them to justify their illegal behavior.

What are some rationalizations?

- The perpetrator is just “borrowing” the stolen assets.
- The perpetrator is not hurting a real person, just a computer system.
- No one will ever know.



Learning Objective 3

Compare and contrast the approaches and techniques that are used to commit computer fraud.



Computer Fraud

- The U.S. Department of Justice defines computer fraud as any illegal act for which knowledge of computer technology is essential for its perpetration, investigation, or prosecution.
- What are examples of computer fraud?
 - unauthorized use, access, modification, copying, and destruction of software or data



Computer Fraud

- theft of money by altering computer records or the theft of computer time
- theft or destruction of computer hardware
- use or the conspiracy to use computer resources to commit a felony
- intent to illegally obtain information or tangible property through the use of computers



The Rise in Computer Fraud

- Organizations that track computer fraud estimate that 80% of U.S. businesses have been victimized by at least one incident of computer fraud.



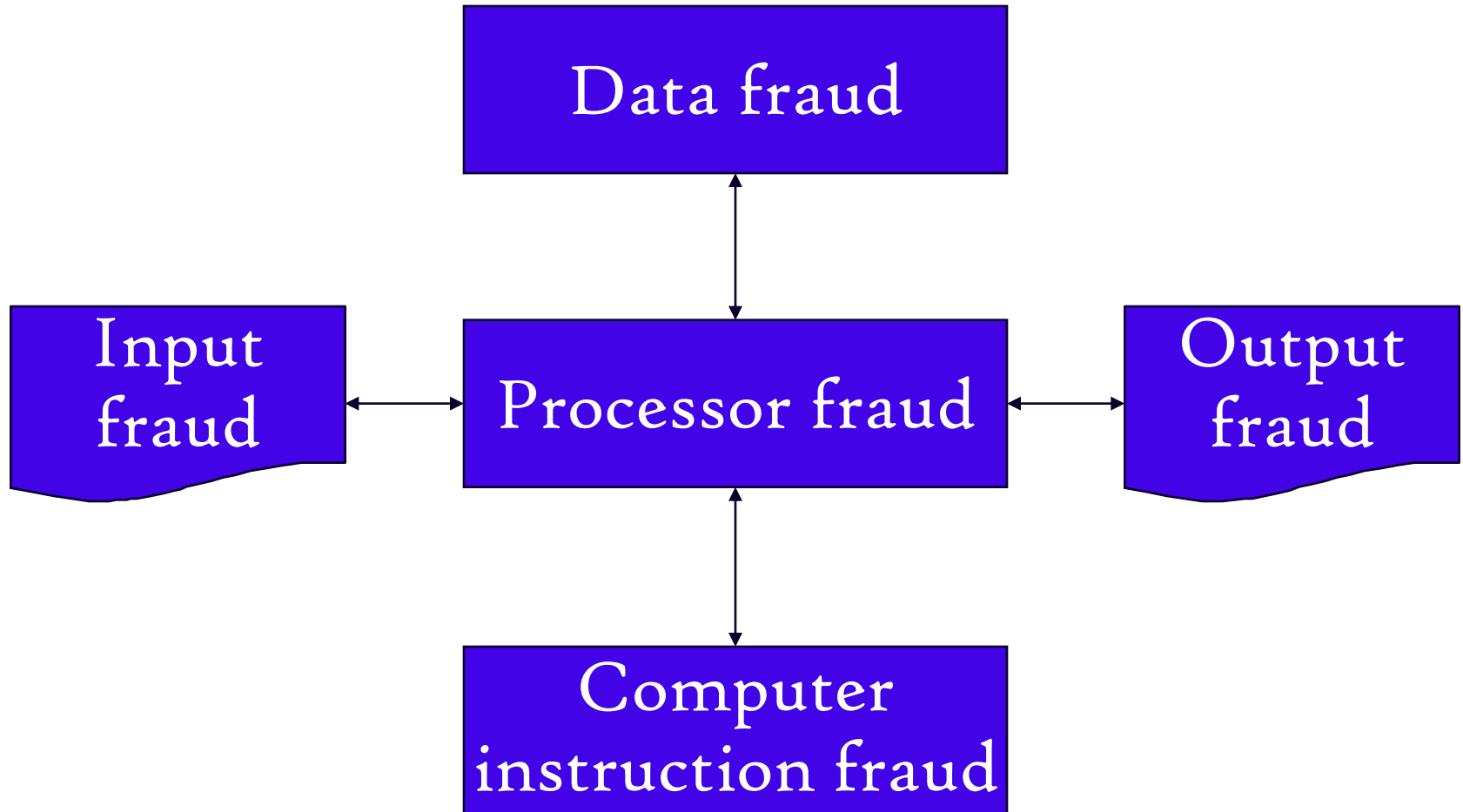
The Rise in Computer Fraud

No one knows for sure exactly how much companies lose to computer fraud. Why?

- There is disagreement on what computer fraud is.
- Many computer frauds go undetected, or unreported.
- Most networks have a low level of security.
- Many Internet pages give instructions on how to perpetrate computer crimes.
- Law enforcement is unable to keep up with fraud.



Computer Fraud Classifications



Computer Fraud and Abuse Techniques

What are some of the more common techniques to commit computer fraud?

- Cracking
- Data diddling
- Data leakage
- Denial of service attack
- Eavesdropping
- E-mail forgery and threats



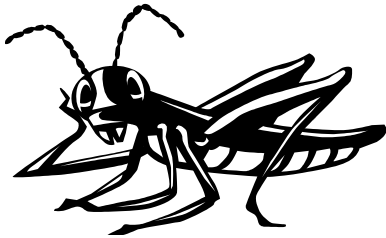
Computer Fraud and Abuse Techniques Contd...



Computer Fraud and Abuse Techniques

- Hacking
- Internet misinformation and terrorism
- Logic time bomb
- Masquerading or impersonation
- Password cracking
- Piggybacking
- Round-down
- Salami technique

Computer Fraud and Abuse Techniques Contd...



Computer Fraud
and Abuse
Techniques

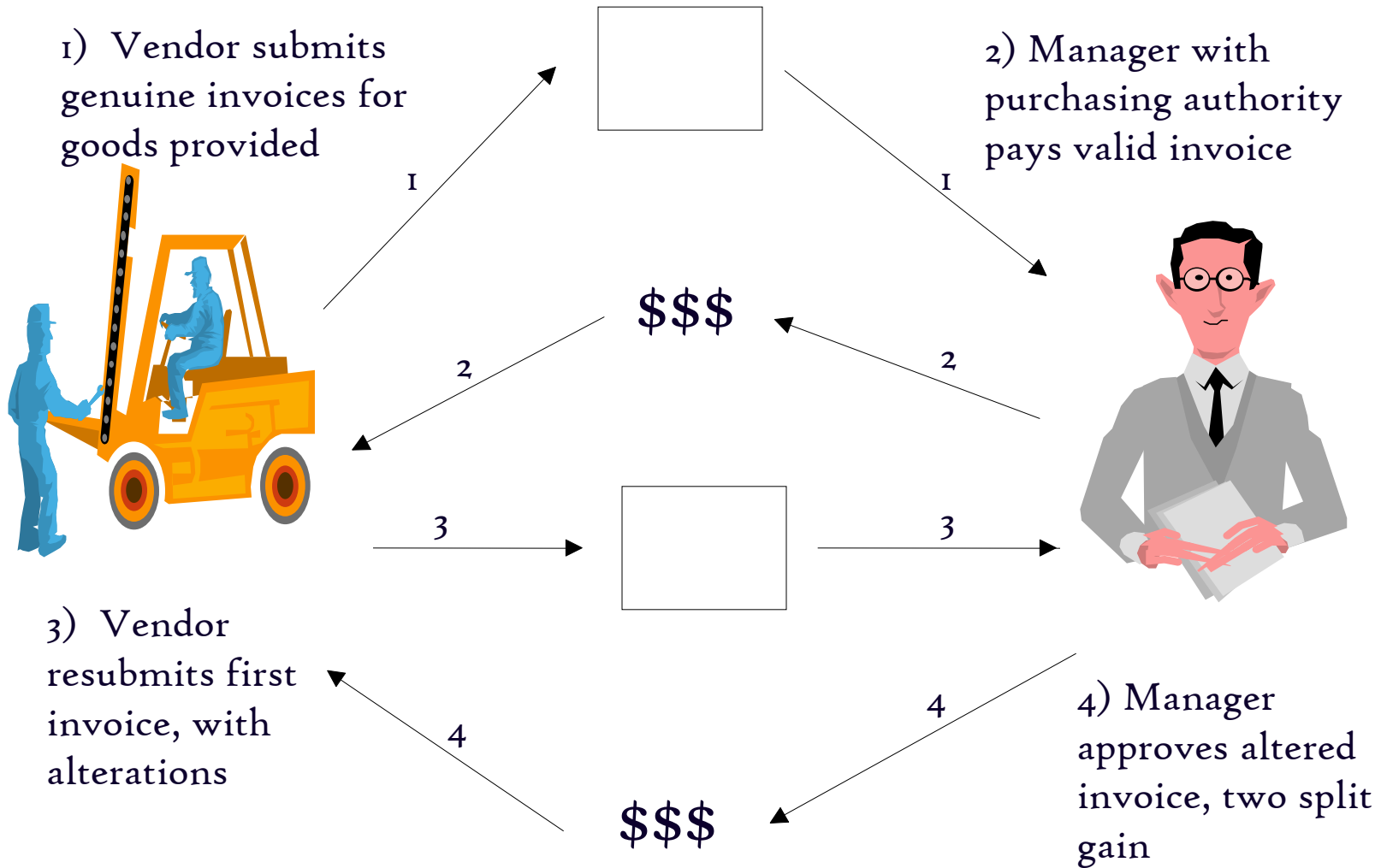
- Software piracy
- Scavenging
- Social engineering
- Super zapping
- Trap door
- Trojan horse
- Virus
- Worm

Objective 4

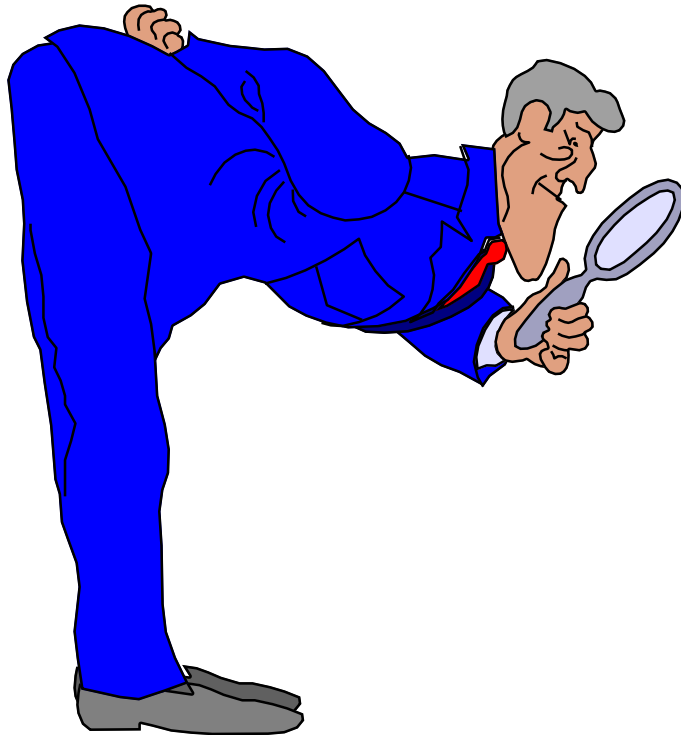
Describe how to deter and detect computer fraud.



Collusion Through Duplicate Invoices



Fraud Detection



- Those analytical and other procedures that enable discovery of anomalies
- Procedures that provide for communication of suspected fraud and illegal acts

Fraud Detection

- Fraud detection involves identifying symptoms that often indicates fraud is being, or has been, committed.
- Fraud investigation, on the other hand, is about examining and studying the symptoms or red flags once identified.
- The computer is one of the most powerful fraud detection tools for the investigator.
- Technology based methods used in fraud detection:
- **i-Inductive fraud detection method**
 - Use of commercial data-mining software, such as Audit Command Language (ACL), to look for anomalies in databases.
- **ii-Deductive fraud detection method**
 - Determine what kinds of frauds can occur in a particular situation and then uses technology and other methods to determine whether those frauds exist.

Fraud Investigation

Once the decision has been made to investigate, the investigation methods that will be used must be determined. In deciding which methods to use, investigators should focus on the strongest type of evidence for the specific fraud.

Fraud investigations are different from audits. In audits we are focusing on the system of internal control. In investigations, we focus on the possible perpetrators or suspects. Internal audits involve interviews, investigations involve interrogations.

When beginning a fraud investigation, it is useful to develop theories about :

What was taken?

Who had opportunity?,

How were assets moved?

How was theft concealed?

How were assets converted?

Red Flag symptoms?

Possible motives : Pressures: Lien, New home, New car, Divorce?

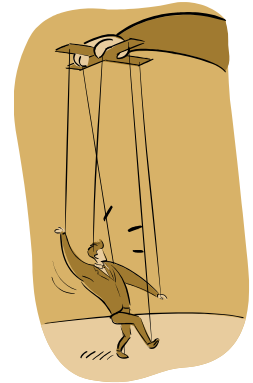
Rationalism: Feels underpaid, Not promoted, Greed?

Opportunity: Lack of or weakness of internal controls?



The whole person

- What element of the individual do you deal with?
- Do you understand him/her?
- What are his/her values?
- Does their status, function, position, dress, office or other affect the manner in which you deal with them?



Theft Investigative Methods

- 1) Surveillance and covert operations
- 2) Invigilation
- 3) Seizing and searching computers
- 4) Physical evidence

Concealment Investigative Methods

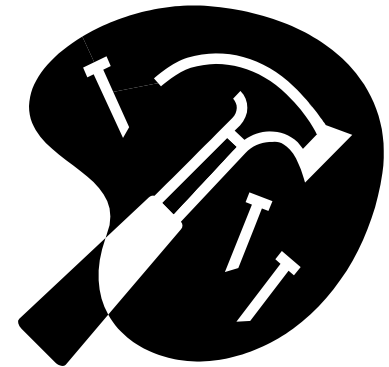
- 1) Document examination
- 2) Audits
- 3) Electronic searches
- 4) Physical asset counts

Conversion Investigation Methods

- 1) Searching Public records- motor vehicles-Land office
- 2) Online resources
- 3) The net worth method

Inquiry Investigative Methods

- 1) Interviews and interrogation
- 2) Honesty testing

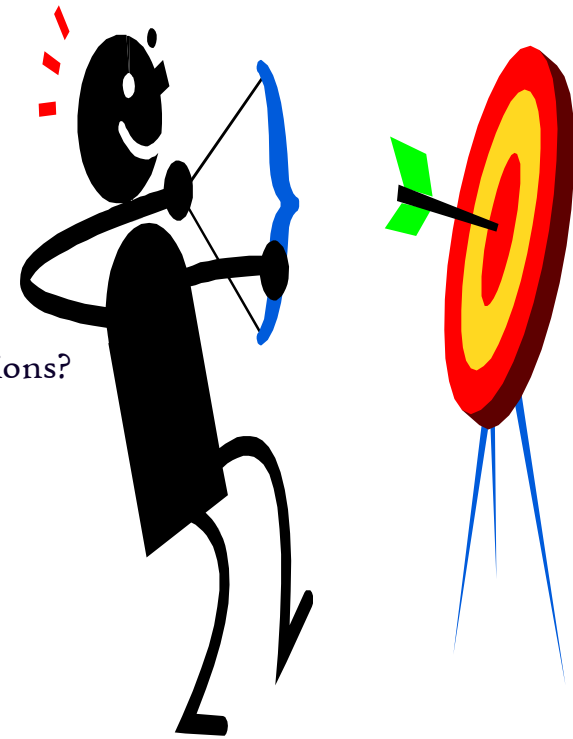


Forensic Auditing

The forensic or fraud auditor is someone who is trained to "think like a crook."

Fraud auditors approach a system with these six questions:

1. What are the weakest links in the system's internal controls?
2. What deviations from good business practices are possible in this system?
3. How are off-line transactions handled, and who can authorize such transactions?
4. What is the simplest way to compromise this system?
5. What controls are subject to override, and who can do it?
6. What is the cultural norm of the work group?



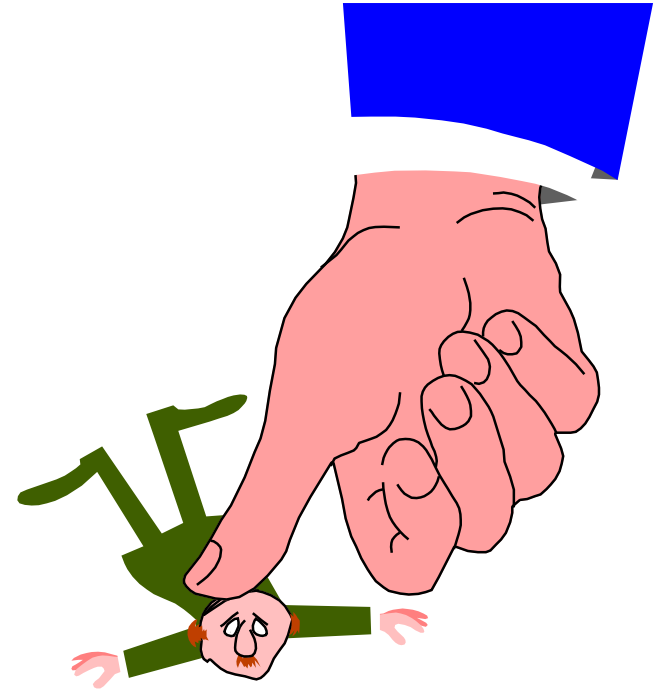
Forensic Auditing (cont)

- In addition to a sound knowledge of business practices, the fraud auditor must be well versed in the operations of the organization in order to quickly seize the evidence needed to prove a fraud.
- The most important skill a fraud auditor can possess is the ability to look at systems and see the exceptions, the oddities, and the irregularities. Things that do not make good sense. In order to recognize these irregular circumstances, the fraud auditor must first know how the system is supposed to work!
- Some people believe that fraud auditors have to be highly intuitive. To that, we would add persistent and personable. Some of the best fraud auditors and investigators can charm people into telling them anything! The fraud auditor needs to be very knowledgeable in human behavioral issues as well as internal control.



The Anti-Fraud Program: The Three Principal Lines of Defense

- First Line - Code of conduct and business ethics policies and procedures
- Second Line - Internal control and Management control structure
- Third Line - Internal audit activities (internal audit presence is a strong deterrent to fraud)



Ethics Policies and Procedures: The First Line of Defense

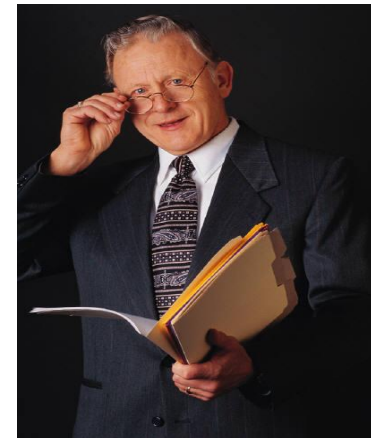
Based on an assessment of the possible risks facing the company, an understandable written employee code of conduct and business ethics document should be in place.



Ethics Policies and Procedures: The First Line of Defense

An Effective Code of Conduct

- Includes Deterrence Elements
- Includes Detection Elements
- Is values based, not rule based
- Has a positive tone, promoting a better workplace
- Requires a fair employer/employee balance



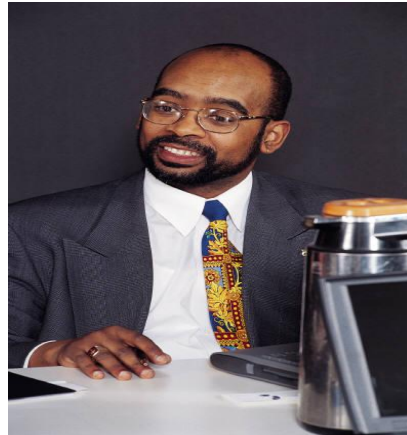
Internal Controls: The Second Line of Defense

- An effective internal control and management organization structure provides both prevention and detection elements, but not significant deterrence!



Internal Audit: The Third Line of Defense

- Internal audit represents a detection line of defense in most companies
 - Operational and internal control reviews
 - Analytical procedures used to isolate anomalies
 - Detail reviews of high control and inherent risk accounts and transactions
- Internal audit does not necessarily represent a deterrence element because of predictability issues



Internal Audit: The Third Line of Defense

- Based on a risk assessment of fraud and illegal acts, internal audit evaluates the 1st and 2nd line defense mitigators
- Key mitigators should be thoroughly tested



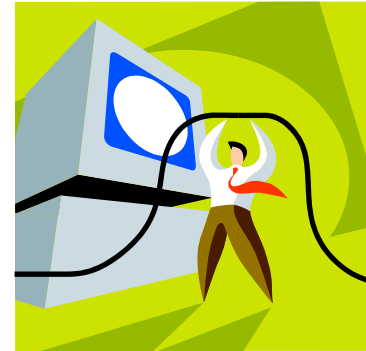
Internal Audit: The Third Line of Defense

- If the mitigators are working effectively, analytical procedures and other tests are needed to isolate and identify any anomalies that may be present
- If no mitigators, or ineffective mitigators, then internal audit must design fraud and illegal act substantive auditing procedures
- In effect, they must search for fraud and illegal acts



Controls that Prevent or Detect Fraudulent Behavior:

1. Control Environment.
2. Accounting System
3. Control Activities
4. Risk Assessment
5. Information and Communication
6. Monitoring



Preventing and Detecting Computer Fraud

What are some measures that can decrease the potential of fraud?

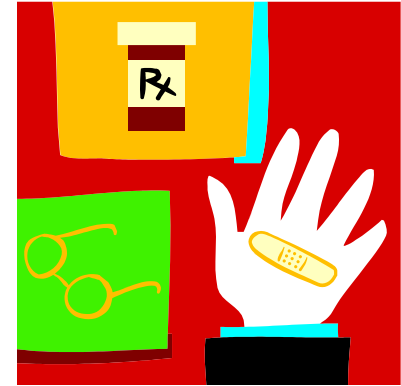
- 1 Make fraud less likely to occur.
- 2 Increase the difficulty of committing fraud.
- 3 Improve detection methods.
- 4 Reduce fraud losses.
- 5 Prosecute and incarcerate fraud perpetrators.



Preventing and Detecting Computer Fraud

1. *Make fraud less likely to occur.*

- Use proper hiring and firing practices.
- Manage disgruntled employees.
- Train employees in security and fraud prevention.
- Manage and track software licenses.
- Require signed confidentiality agreements.



Preventing and Detecting Computer Fraud

2. Increase the difficulty of committing fraud.

- Develop a strong system of internal controls.
- Segregate duties.
- Require vacations and rotate duties.
- Restrict access to computer equipment and data files.
- Encrypt data and programs.



Preventing and Detecting Computer Fraud

3. *Improve detection methods.*

- Protect telephone lines and the system from viruses.
- Control sensitive data.
- Control laptop computers.
- Monitor hacker information.



Preventing and Detecting Computer Fraud

4. *Reduce fraud losses.*

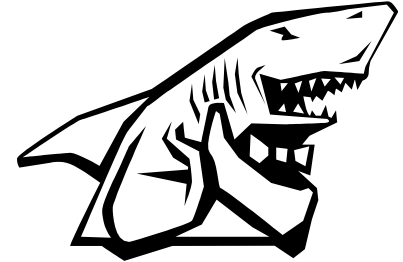
- Maintain adequate insurance.
- Store backup copies of programs and data files in a secure, off-site location.
- Develop a contingency plan for fraud occurrences.
- Use software to monitor system activity and recover from fraud.



Preventing and Detecting Computer Fraud

5. Prosecute and incarcerate fraud perpetrators.

- Most fraud cases go unreported and unprosecuted. Why?
 - Many cases of computer fraud are as yet undetected.
 - Companies are reluctant to report computer crimes.



E&Y Fraud Survey – Key Findings

In the last year :

- 2 in 3 had been defrauded
- 1 in 10 had more than 50 frauds
- 82% were committed by employees
- Half of the employees had over 5 years service
- A quarter had more than 10 years service
- A third of the frauds were by management
- Only 29% of losses were recovered



Percentage of Cases of Top Frauds Reported by Size of Organization

Method	Up to 100 Staff	100+ Staff
Billing	28.7%	24.9%
Check Tampering	26.1%	8.0%
Corruption	26.5%	35.2%
Skimming	21.6%	11.0%
Expense Reimbursement	16.8%	14.2%
Non-Cash	14.9%	18.1%
Cash on Hand	14.7%	10.7%
Payroll	13.4%	6.5%
Larceny	12.3%	8.4%
Financial Statement	5.6%	4.5%
Register Disbursement	3.0%	2.9%

Effectiveness of Detection Methods

Effectiveness of Detection Methods	
Detection Method	Per Cent of Cases
Tip	40.2
Management Review	15.4
Internal Audit	13.9
Accidental	8.3
Account Reconciliation	6.1
Document Examination	5.2
External Audit	4.6
Surveillance/Monitoring	2.6
Notified by Police	1.8
Confession	1.0
IT Controls	0.8



Business
Wisdom
for
Today's
Economy

"Tips have consistently been the most common way to detect fraud Such systems enable employees to anonymously report fraud or misconduct by phone or through a web-based portal. [Anonymity] is key because employees often fear making reports due to the threat of retaliation from superiors or negative reactions from their peers. ... In organizations that had hotlines, 47 per cent of frauds were detected by tips, while in organizations without hotlines, only 34 per cent of cases were detected by tips."

-- Report to the Nations on
Occupational Fraud and Abuse

Combating Fraud

1. Call it Fraud
2. Get Executive Buy-In
3. Tell the World
4. Look for Current Cases
5. Investigate and Prosecute all Cases
6. Get Publicity



The Courtenay Thompson Four Step Approach to Fraud Prevention includes:

1. Screen out those who are likely to commit fraud.
2. Reduce the opportunity available.
3. Create an environment in which employees believe that dishonest acts will be detected by management, monitoring techniques, other employees, or the auditors.
4. Create an environment in which dishonest acts are not tolerated and are, in fact, punished.

Fraud Fighting Skills

1-**Analytical skills:** it requires significant amounts of diagnostic and exploratory work to discover what is really happening.

2- **Communication skills:** A good communicator will know how hard to push for evidence and confessions, structure questions and interviews and write reports that are valued by courts, lawyers and others.

3-**Technology skills:** technology allows fraud examiners to analyze huge databases quickly.

Additional skills include:

- -Understanding of accounting and business
- -Knowledge of civil and criminal laws, and other legal fraud-related issues
- -Knowledge of human behavior (psychology)
 - Keep your eyes and ears open:
 - Develop observation skill and observe overnight radical changes.
 - Do not ignore hearsay things. Keep in the parking folder.
 - Develop professional skepticism.
 - Develop skills to observe unusual behavioral activities.
 - Develop skills to observe body language.



Conclusion

- Strictly enforce existing controls.
- Employees should be trained in fraud awareness, security measures, and ethical issues.
- Ensuring the existence of control with systems designed to prevent or deter the forms of fraud.
- Identifying areas of risk where theft or manipulation may be likely to occur.
- Ensuring adequacy and effectiveness of controls in financial accounting and other areas subject to theft, fraud or embezzlement.
- Exercising the care and skill of a reasonably prudent and competent professional.
- Have a hotline with recording machine. The tipper should be allowed to report not necessarily in his own voice.
- Website portals that are not asking for email address or telephone numbers of the reporter.

