

MIS 5121:Enterprise Resource Planning Systems  
Week 3: *Fraud, Procure to Pay Process Controls*

# Reading Assignment Questions:

- Did others find the reading and table codes very confusing this week?

# Control Failure: ACL Technologies, Inc.



- Background:

- ❖ Subsidiary of United Industrial Corporation (UIC)
- ❖ 1990's Sought gov't contracts to build F-16 combat aircraft depots in Egypt
- ❖ Contracts: \$64 million in revenue, \$8.6 million in net profit 1999 and 2004
- ❖ Retained services of retired EAF General (the "EAF Agent") knowing that he had connections to EAF officers – beneficiaries of depot

- Control Failures: contract awarded in 2002

- ❖ 'Agent' and ACL President discussed funds to 'start give motivation'
- ❖ *Front-end:* Subsidiary head authorized large payments without meaningful substantiation, supporting documents (segregation of duties)
- ❖ *Back-end:* Paid 'Agent' for 'consulting' and 'marketing' services with no meaningful records documenting the services
- ❖ *Agent due diligence:* initially no contract, contract not reviewed by legal, used form submitted by agent without review
- ❖ *Contractual Rights:* contracts without gov't required audit rights to review 'agent' activities (e.g. no supervision of activities).



# Control Failure: ACL Technologies, Inc.

- Results / Outcomes:

- ❖ SEC books & records and internal controls charges against the parent company
  - ❖ Liability transferred to parent company: UIC routinely identified the ACL President as a member of UCI's senior management, indicating the degree of control it possessed
- ❖ SEC 'read between the lines' to charge with violating Foreign Corrupt Practices Act (FCPA) anti-bribery provisions (SEC will impute culpable knowledge or willful blindness to a parent corporation based on the internal control failures).
- ❖ UIC's settled out of court (2009):
  - ❖ "neither admitting nor denying" the allegations
  - ❖ Fine of approximately \$340,000 (from contract net profit of \$9,000,000)
  - ❖ Cease-and-desist order requiring to follow what the law requires anyway



- References / Links:

- ❖ [http://www.shearman.com/~media/Files/NewsInsights/Publications/2009/06/Internal-Control-Failures-Lead-to-Parent-Liability/Files/Click-here-to-view-memo-Internal-Control-Failure\\_/FileAttachment/FCPA060209InternalControlFailuresLeadtoParentLia\\_\\_.pdf](http://www.shearman.com/~media/Files/NewsInsights/Publications/2009/06/Internal-Control-Failures-Lead-to-Parent-Liability/Files/Click-here-to-view-memo-Internal-Control-Failure_/FileAttachment/FCPA060209InternalControlFailuresLeadtoParentLia__.pdf)

External Financial Reporting regulations

Other Reg's

Organization's  
Objectives & Policies

Balance  
Sheet

P & L

Notes

FDA etc.

Performance & Policies

Arise through

Must be observed / achieved in

### Business Processes

Procurement

Production

Order to \$\$

Finance

IT

Quality

Logistics

HR

...

Contain

Assertions

- Completeness
- Existence, rights
- Accuracy
- Valuation
- Presentation

Risks

- Product quality
- Delivery (OTD)
- Unused capacity
- Excess Costs
- Lower Sales

Errors & Fraud

Minimized by

### ISC framework in the ERP environment

- Entity level controls
  - Automated application controls
- Manual and semi-automated business process controls
- Authorizations and access protection (confidentiality, integrity)
- IT General controls (change management, operation, security)
- Automated testing and monitoring of business processes, KPIs, etc.

External Financial Reporting regulations

Other Reg's

Organization's  
Objectives & Policies

Balance  
Sheet

P & L

Notes

FDA etc.

Performance & Policies

Arise through

Must be observed / achieved in

Business Processes

Procurement

Production

Order to \$\$

Finance

IT

Quality

Logistics

HR

...

Contain

**Assertions**

- Completeness
- Existence, rights
- Accuracy
- Valuation
- Presentation

Risks

- Product quality
- Delivery (OTD)
- Unused capacity
- Excess Costs
- Lower Sales

Errors & Fraud

Minimized by

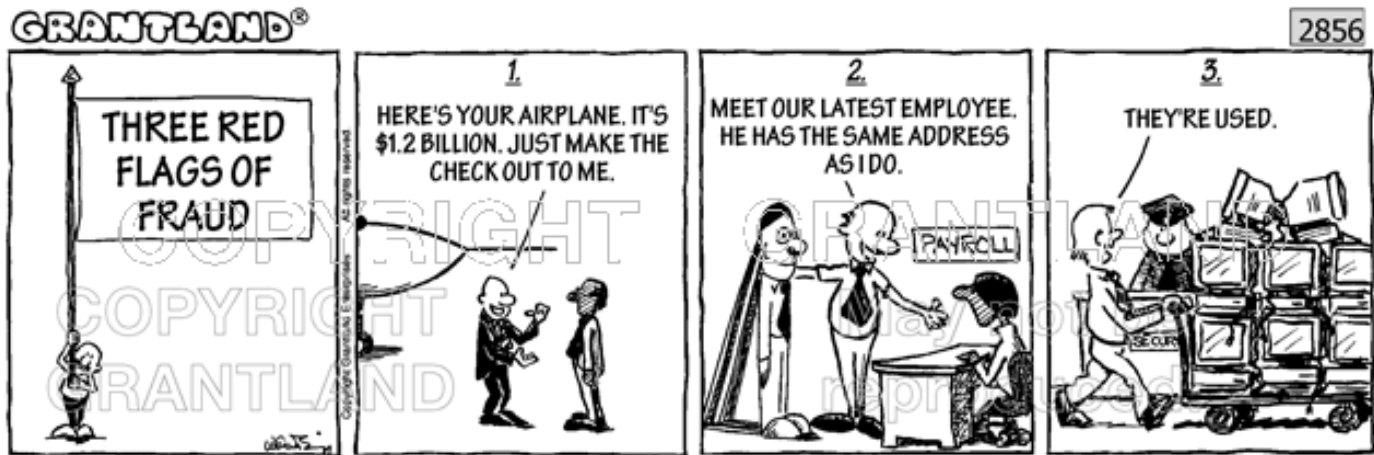
### ISC framework in the ERP environment

- Entity level controls
  - Automated application controls
  - Manual and semi-automated business process controls
- Authorizations and access protection (confidentiality, integrity)
- IT General controls (change management, operation, security)
- Automated testing and monitoring of business processes, KPIs, etc.

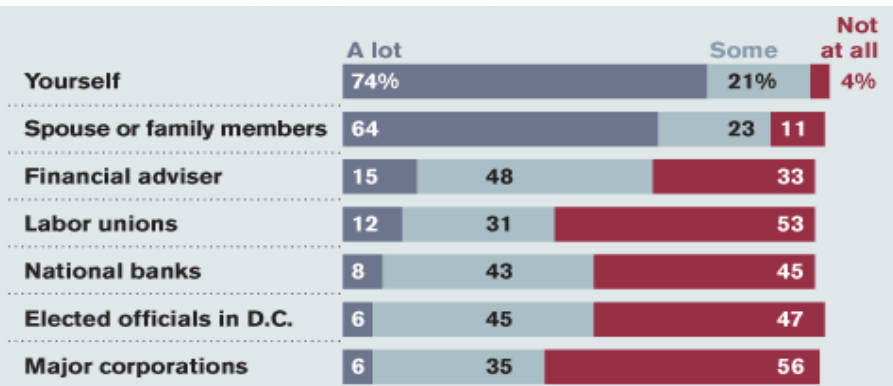
# Fraud

## Definition

‘deception (misrepresentation or omission)  
deliberately practiced in order to secure  
unfair or unlawful gain’



# Whom do you trust?

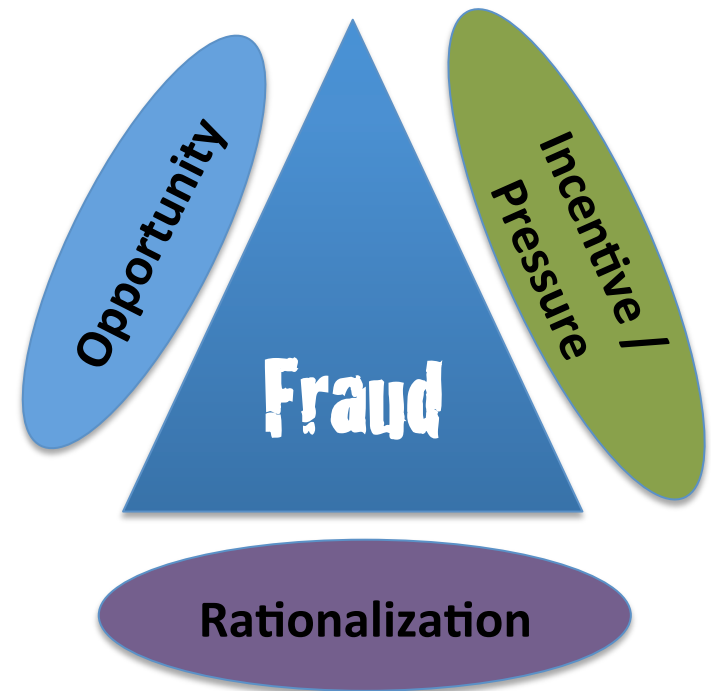




# Environment Favorable to Fraud

Framework for spotting high-risk situations

- Perceived **opportunity** (*I can do it / conceal it and not get caught*)
  - Poor internal controls
  - Lack of oversight
- **Incentive or Pressure** (*Financial or emotional force pushing to commit fraud*)
  - Meet expectations
  - Avoid criticism
  - Cover a mistake
  - Personal failures, needs
- **Rationalization** (*Personal justification for dishonest actions*)
  - Low compensation
  - Company is profitable



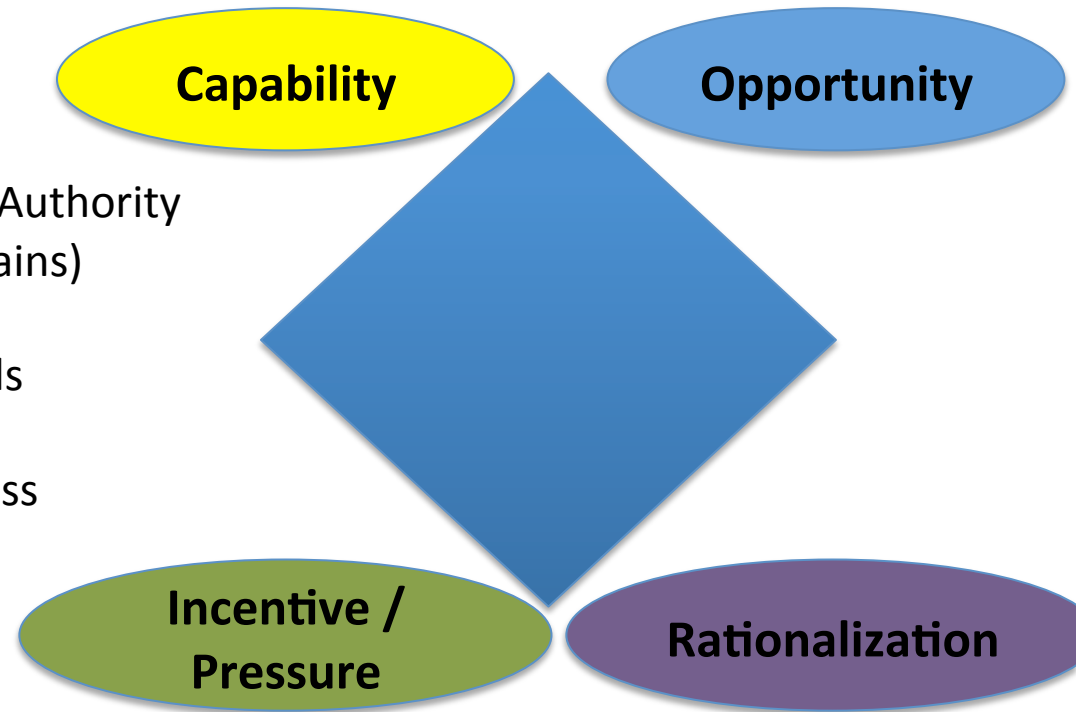
Fraud Triangle

# The Fraud Diamond

Framework for spotting high-risk situations

- **Capability**

- Position / Organizational Authority
- Knowledge of System (brains)
- Confidence / ego
- Persuasive / coercion skills
- Deceptive nature (*liar*)
- Resilient /immune to stress



# Occupational Fraud Categories

- Asset Misappropriation:
  - Perpetrator steals or misuses an organization's resources
- Corruption:
  - Use his / her influence in business transactions
  - Method violates duty to employer
  - Obtains benefit for themselves or a partner)
- Financial Statement Fraud:
  - Intentional misstatement or omission of material information in organizations financial reports



	Andhra Pradesh	Andhra Pradesh	Research/Spices
		Apartment	Service Center
OPERATING REVENUES AND SUPPORT	\$1,025,883	\$4,477,086	—
Operating	5,016,272	3,595,389	—
Support	902,208	749,804	—
Operating & Support	964,480	41,309	—
Operating & Support	1,683,837	30,581	—
Operating & Support	—	2,267,778	—

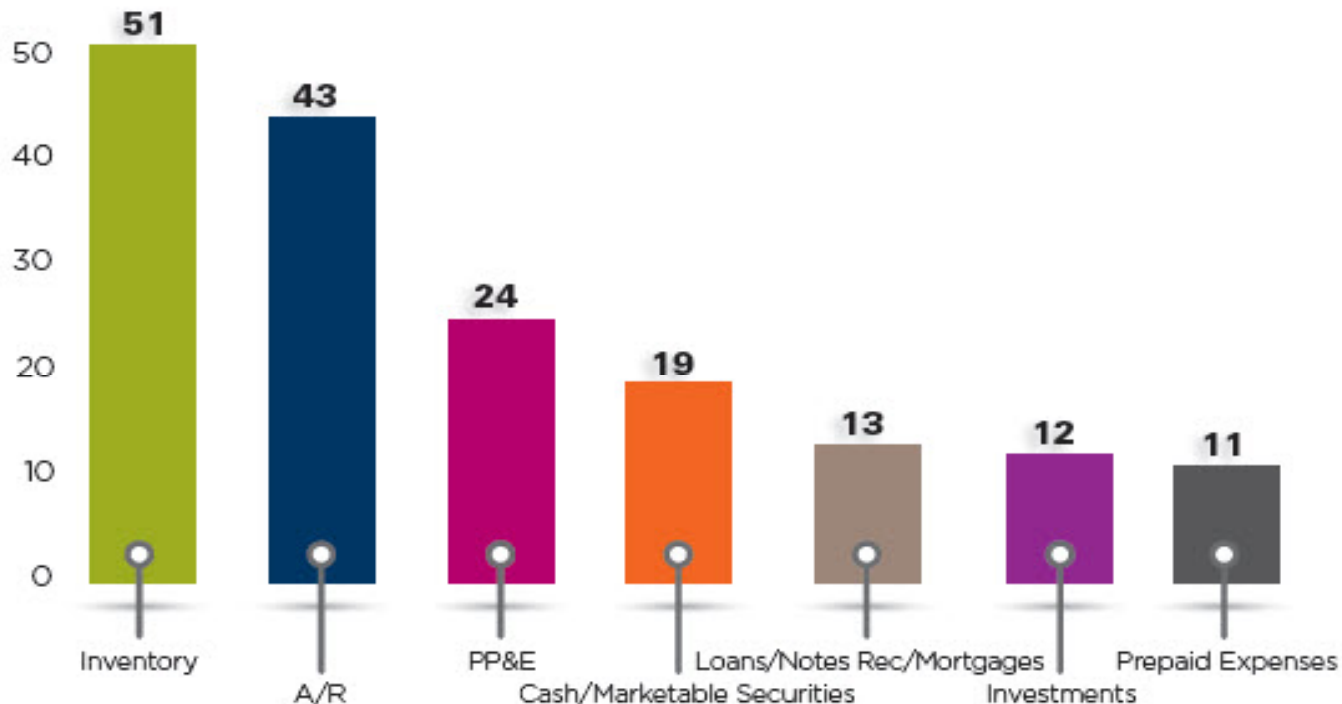
Source: Association of Certified Fraud Examiners – 2010 Report to the Nation

Balance Sheet	
As at 31 December 2005	
Notes	2004
10	2005
11	2006
12	2007

# Most Common Fraud Techniques

- Improper revenue recognition (61% of cases vs. 50% in previous study)
- Overstatement of assets/capitalization of expenses (51%)

Number of Fraud Cases With Asset Accounts Misstated



# Most Common Fraud Techniques

- Understatement of expenses/liabilities (31%)
- Other techniques such as acquisitions, JVs, netting of amounts (20%)
- Disguised through use of related parties (18%)
- Misappropriated assets (14%)



# Case Example – Employee Embezzlement

- Company with annual revenues of approximately \$20 – 30 million
- Payroll clerk develops a scheme to misappropriate cash through fraudulent expense reimbursements
  - Establishes fictitious employee names and links her checking account to the payroll records for direct deposit
  - The clerk submits fraudulent expense reimbursements
  - The misappropriated funds were moved out of the checking account via a series of transactions initiated to launder the cash
- Over five years she stole over \$5 million
- Pled guilty to grand larceny and money laundering. Received a three year prison sentence and was subsequently deported to her native Italy



# Case Example – Employee Embezzlement

- Pressure / incentive
  - Gambling
  - Living beyond her means
  - Desire to keep up façade to family and friends
- Perceived opportunity
  - No internal controls
  - No oversight by management
  - No applicant screening program
  - No segregation of duties
- Rationalization
  - I deserve more than I am being paid
  - I am not hurting anyone



# Case Example – Vendor Kickback

- Company with annual revenues of \$3 – 5 billion
- Facilities management members willfully participate in bribery scheme with two vendors for receiving contracts and approval of fictitious invoices
  - Vendors would inflate costs of materials by more than 1,000% and submit fictitious invoices to support costs. Contracts were for 0% markup on materials
  - Vendors would charge company prevailing wage for workers time and pay workers far less, pocketing the difference
  - Members of facilities management received cash, services on personal homes and gifts
- Loss to the company was approximately \$18 million for overbilling of services
- Vendors and management involved pled guilty to crimes including bribery, grand larceny, and money laundering; sentences ranged from probation to prison terms as well as restitution





# Case Example – Vendor Kickback

- Pressure / incentive
  - Living beyond means
  - Requirement to lower costs
- Perceived opportunity
  - Weak internal controls
  - No oversight by management
  - Ignoring of red flags
  - No segregation of duties
- Rationalization
  - I harm, no foul

KICKBACK =

- Bonus*
- Commission**
- Compensation
- Gift*
- Gratuity*
- Incentive
- Referral Fee*
- Thank You*

# Fraud: Personal Knowledge Scenarios

## Example 1

- Business Segment manager
  - Member of acquired company (~ 1 year prior)
  - Recently promoted to job with significant responsibility
  - Highly respected, future potential individual
- Fired and arrested for Fraud
  - Filed travel expense statements that included fictitious expenses
  - Many instances over several years (at current company and before acquisition)
  - Members of facilities management received cash, services on personal homes and gifts



# Fraud: Personal Knowledge Scenarios

## Example 2

- Regional Supply Chain Manager and his Assistant
  - Long tenure at company
  - Highly respected, feared manager
  - Lead supply chain network of 12+ plants in US, Canada
- Fired
  - Supposedly: in conjunctions with 1+ persons at plants included family members in part time pay
  - Payments for no work



## Example 3

- Senior IT Manager
  - Leader of largest project in company – just promoted
  - Highly respected, influential leader
- Fired and arrested for Fraud
  - During large acquisition shared insider information about acquisition with stockbrokers
  - Stockbroker along with family members used information to make stock positions
  - Stock positions taken were in wrong direction (bet on stock increasing, it tanked)



# Real World Examples – From Class

- 
- 
- 
- 
-

# Reading Assignment Questions:

- Which of the three factors of the fraud triangle is the one that leads people to perform unethical actions in a company?
- I confuse how SAP system detects fraud when it sets the authorizations to control the changes. It sounds to simple.
- Managers have power to employ control mechanisms, and auditor has special knowledge to identify control weakness Which one of those are legally responsible if a fraud happens?
- What types of fraud risks are highest priority for an organization?
- What are some ways to combat collusion among employees within an ERP system, if any?

# Asset Misappropriation Fraud Schemes

Category	Description	Examples	% cases
Billing	Causes employer to issue payment by submitting invoices for fictitious goods or services, inflated invoices or invoices for personal purchases	Employee creates a shell company and bills employer for services not actually rendered	26.0 %
Non-Cash	Employee steals or misuses non-cash assets of the organization	Employee steals or misuses non-cash assets of the Organization steals or misuses confidential customer financial information	16.3 %
Revenue Reimburse	Employee makes a claim for reimbursement of fictitious or inflated business expenses	Employee files fraudulent expense report, claiming personal travel, etc.	15.1 %
Skimming	Cash is stolen from an organization <b>before</b> it is recorded on the organization's books and records	Employee accepts payment a customer, but does not record the sale, and instead pockets the money	14.5 %
Check tampering	Person steals his employer's funds by intercepting, forging, or altering a check drawn on one of the organization's bank accounts	Employee steals blank company checks and makes them out to himself or an accomplice	13.4 %
Cash on Hand	Perpetrator misappropriates cash kept on hand at the victim organization's premises	Employee steals cash from a company vault	12.6 %
Cash Larceny	Cash is stolen from an organization <b>after</b> it is recorded on the organization's books / records.	Employee steals cash and checks from daily receipts before they can be deposited in the bank	9.8 %
Payroll	Employee causes his employer to issue a payment by making false claims for compensation	Employee claims overtime for hours not worked or adds ghost employees to the payroll	8.5 %
Cash Register	Person makes false entries on a cash register to conceal fraudulent removal of cash	Employee voids a sale on the cash register and steals the cash	3.0 %

T2928

# GRANTLAND®

I JUST FINISHED THAT  
COURSE ON FRAUD.

HOW WAS  
IT?

GREAT! THEY SHOWED  
US ALL SORTS OF WAYS  
TO MAKE MONEY.

Copyright © Grantland Enterprises. All rights reserved.

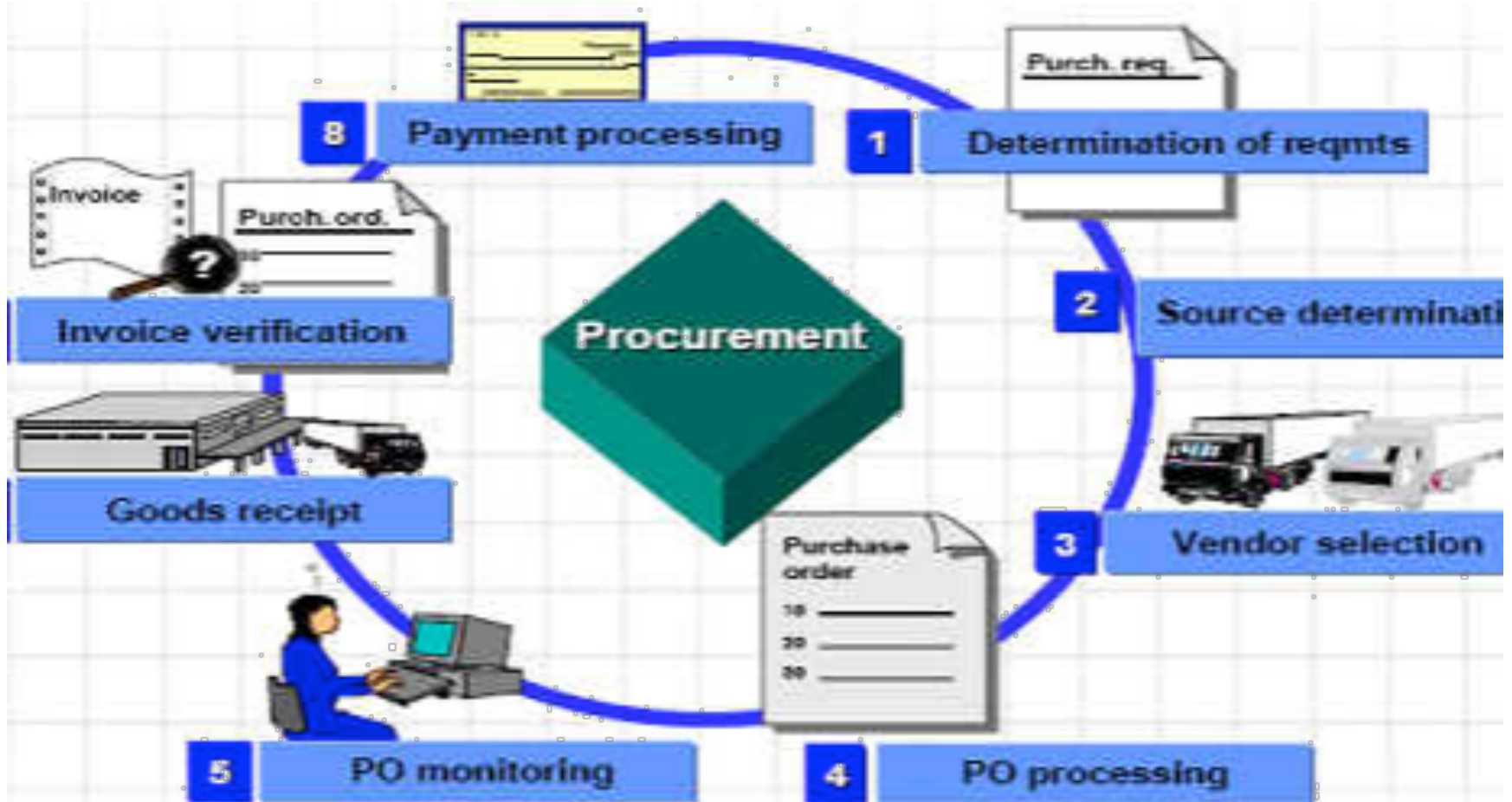
COPYRIGHT  
GRANTLAND

# Business Process Controls

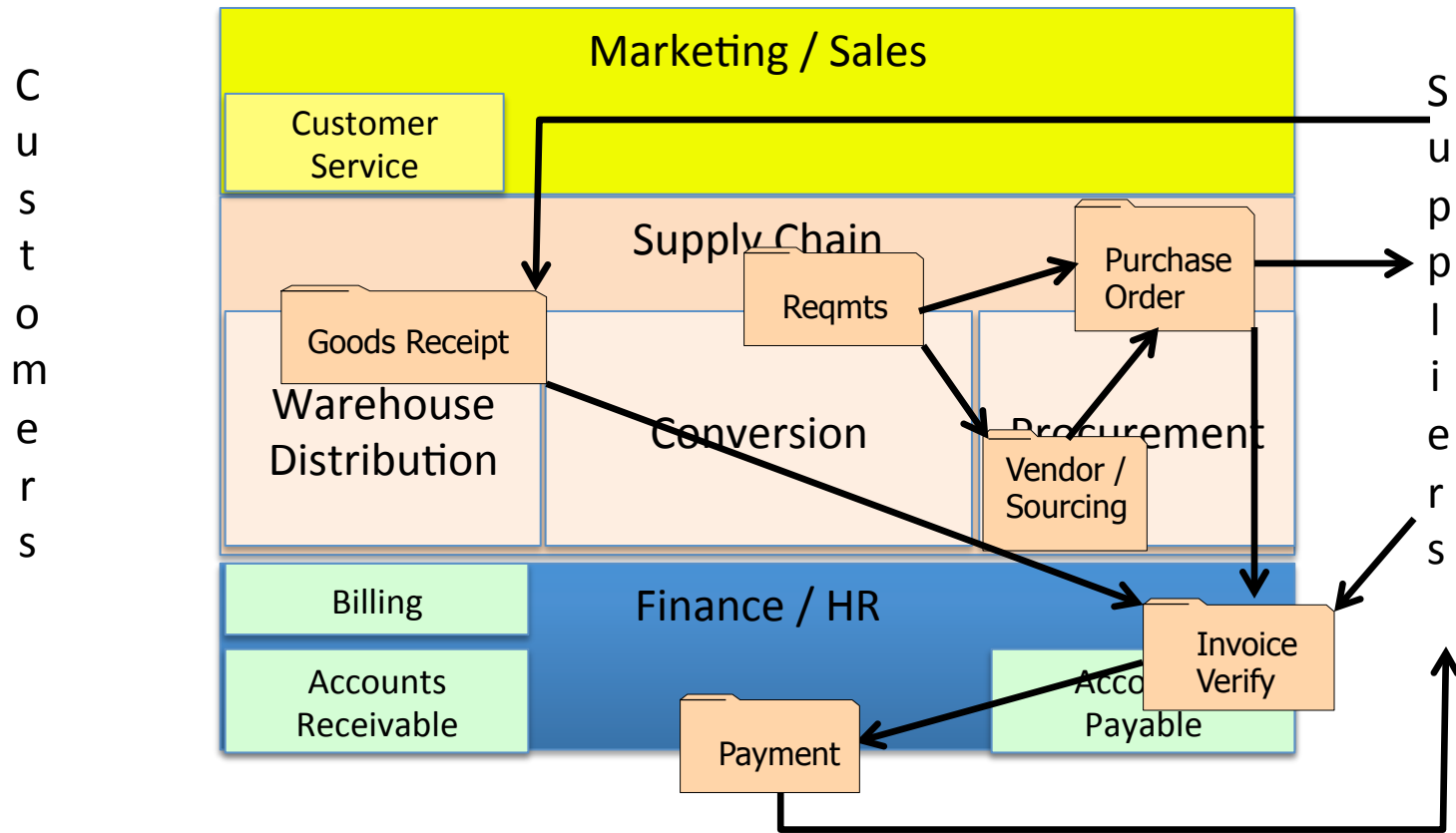
## Procure to Pay



# Procurement Process



# Procurement at GBI



# The Many Flavors of Procurement

What Does Global Bike, Inc. Procure?



- 
- 
- 
- 
- 
-

# The Many Flavors of Procurement

- Materials / Raw Materials
- Labor Services
- Other Services
- Leases / Rentals
- Supplies (Office, Maintenance, Production, ...)
- Logistics
- Information Technology
- No PO
- Inter-company vs. 3<sup>rd</sup> Party
- Acquisitions

# Class Exercise

- Small groups – Assigned sub-process
  1. Vendor Selection and source determination
  2. Purchase Order (PO) Processing
  3. Goods Receipt
  4. Invoice Verification / Payments
- Assignment:
  - List 5 Risks that might exist in assigned sub-process
  - For 1 of the risks – define a control to minimize the risk
- 8 Minutes

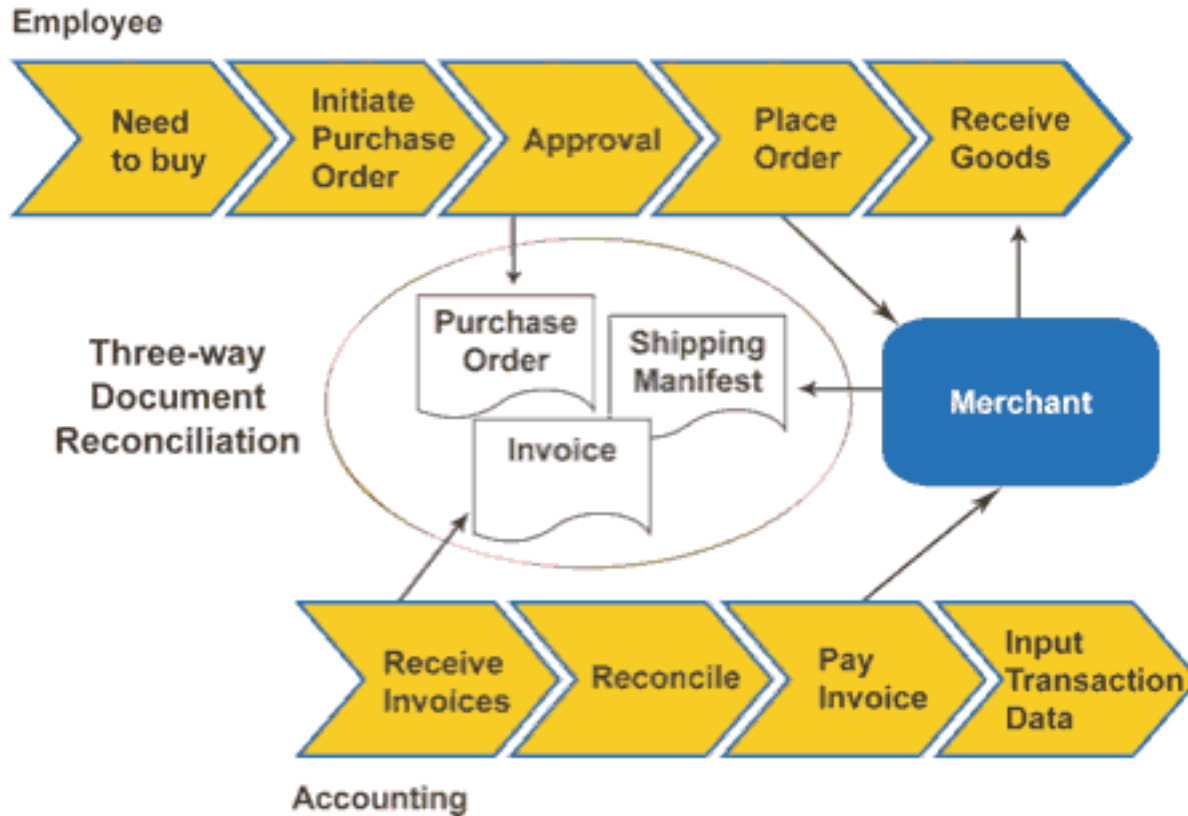
# Report Back



# Procure to Pay: Common Risks

- Creation of fictitious vendors, purchase orders and service/good receipt
- Purchases not correctly Authorized
- Delivery address modification
- Import / export control violations
- Inadequate price negotiation
- Quality of goods / services received
- Inventory manipulation
- Modification of vendors payment information
- Records lost / destroyed
- Manipulation of client names and addresses on vouchers / refund
- Price increase in purchase orders (to establish a kickback program)
- Over / under charged workload / hours / costs
- Wrong payments / duplicate payments
- Approval of fictitious travel expenses

# Controls: 3-way Match





# Procure to Pay: Common Controls

- Segregation of Duties
- Purchasing policies (Written, taught, monitored)
- Contract / PO approvals
- Vendor / source / price Decisions Monitored
- Avoid Advance payments
- Invoices to A/P
- Monitor GR / IR Account
- Return Procedures (written, taught, monitored)
- Supplier / Procurement independence
- PO revisions monitored / controlled
- No PO payments avoided / controlled
- 3-way Match used where possible

# Reading Assignment Questions:

- How can SAP processes decrease chance of fraud where we create vendors who are not vendors or someone credits the account for payments that were never actually received?
- Last class noted all purchasing orders cannot be deleted. Is that a preventative control to fraud because fictitious orders cannot be deleted and can be referred to in the future?

# Reference

- [Checklist: Standards of Internal Control for Purchasing and Ordering \(Institute of Finance & Management\)](#)
-

# Break Time





# Purchase-to-Pay Exercise



- Primary Learning objectives
  - Experience the steps in a typical purchasing transaction
  - See how an ERP system handles typical purchasing transactions
  - Work through the procedures involved in a test of transactions
  - Investigate related application controls in an ERP system
- Secondary learning objectives:
  - See the integration between materials management (MM) and financial accounting (FI) modules of SAP
  - View some basic FI module settings than enable proper system functions



# Exercise 1: Purchase to Pay



- Agenda
  - Last Class (*Jan 28*): Logging On; Steps 1 - 6
  - This Class (*Feb 2*): Steps 7 - 14
  - *Due Feb 5 11:59 PM*: Assignment Submission



# Exercise 1: Purchase to Pay



- Task 7 – Create a Purchase Order to Buy the Trading Good
  - Menu: **Logistics** ▶ **Materials Management** ▶ **Purchasing** ▶ **Purchase Order** ▶ **Create** ▶ **Vendor/Supplying Plant Known**
  - Transaction: **ME21N**
- Task 8 - Check Status of Various Accounts
  - Check Inventory: MM Inventory Quantity  
Transaction: **MMBE** (*Stock Overview*)
  - Check GL Inventory, GL Cash, GL A/P, GR/IR (Goods Received / Invoice Received):  
Transaction: **S\_ALR\_87012291** (*Line Item Journal*)
  - Check A/P Vendor sub-ledger:  
Transaction: **FBL1N** (*Vendor line item display*)

# Exercise 1: Purchase to Pay



- Task 9 – Receive the Product from the Vendor
  - Menu: *Logistics* ▶ *Materials Management* ▶ *Inventory Management* ▶ *Goods Movement* ▶ *Goods Receipt* ▶ *For Purchase Order* ▶ *PO Number Known*
  - Transaction: **MIGO**
- Task 10 - Check Status of Various Accounts
  - See details of Task 8
- Task 11 – Receive the Invoice from the Vendor
  - Menu: *Logistics* ▶ *Materials Management* ▶ *Purchasing* ▶ *Purchase Order* ▶ *Follow-on Functions* ▶ *Logistics Invoice Verification*
  - Transaction: **MIGO**





# Exercise 1: Purchase to Pay



- Task 12 - Check Status of Various Accounts
  - See details of Task 8
- Task 13 – Make the Payment to the Vendor
  - Menu: **Accounting** ▶ **Financial Accounting** ▶ **Accounts Payable** ▶ **Document Entry** ▶ **Outgoing Payment** ▶ **Post**
  - Transaction: **F-53**
- Task 14 - Check Status of Various Accounts
  - See details of Task 8
- Task 15 – Write down the system-generated journal entries
  - Non-SAP task

# Extra Slides



# Exercise 1: Purchase to Pay



- Task 6 - Check Status of Various Accounts
  - Check Inventory: MM Inventory Quantity  
Transaction: **MMBE** (*Stock Overview*)
  - Check GL Inventory, GL Cash, GL A/P, GR/IR (Goods Received / Invoice Received):  
Transaction: **S\_ALR\_87012291** (*Line Item Journal*)
  - Check A/P Vendor sub-ledger:  
Transaction: **FBL1N** (*Vendor line item display*)