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 imputed 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:**
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.
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?

<table>
<thead>
<tr>
<th></th>
<th>A lot</th>
<th>Some</th>
<th>Not at all</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yourself</td>
<td>74%</td>
<td>21%</td>
<td>4%</td>
</tr>
<tr>
<td>Spouse or family members</td>
<td>64%</td>
<td>23%</td>
<td>11%</td>
</tr>
<tr>
<td>Financial adviser</td>
<td>15%</td>
<td>48%</td>
<td>33%</td>
</tr>
<tr>
<td>Labor unions</td>
<td>12%</td>
<td>31%</td>
<td>53%</td>
</tr>
<tr>
<td>National banks</td>
<td>8%</td>
<td>43%</td>
<td>45%</td>
</tr>
<tr>
<td>Elected officials in D.C.</td>
<td>6%</td>
<td>45%</td>
<td>47%</td>
</tr>
<tr>
<td>Major corporations</td>
<td>6%</td>
<td>35%</td>
<td>56%</td>
</tr>
</tbody>
</table>
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

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

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

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 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 too 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

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

Source: Association of Certified Fraud Examiners – 2010 Report to the Nations on Occupational Fraud and Abuse – Global Fraud Study
I just finished that course on fraud.

How was it?

Great! They showed us all sorts of ways to make money.
Business Process Controls

Procure to Pay
Procurement Process

1. Determination of reqmts
2. Source determination
3. Vendor selection
4. PO processing
5. PO monitoring
6. Goods receipt
7. Invoice verification
8. Payment processing
Procurement at GBI

Marketing / Sales
- Customer Service

Warehouse Distribution
- Goods Receipt

Conversion
- Reqmts
- Vendor / Sourcing

Procurement
- Purchase Order

Finance / HR
- Invoice Verify
- Accounts Payable

Billing
- Accounts Receivable

Payment

Customer / Suppliers
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
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)*