Proactive Fraud Detection with Data Mining
“Fear not the computer – You play ball with it and it will play ball with you”

Executive Summary
The time to test fraud controls is before you have a fraud [anti-fraud assessment]. How strong are your controls? Are you looking for fraud or is fraud looking for you? The longer it takes to detect fraud the lower the chance for recovery and the higher the cost of damages.

“Proactive” vs. “Reactive” Preemptive message of ACFE

Ongoing Monitoring
Governance “Tone at the Top”
Controls Testing “Looking for Fraud”
Incident Response “Suspected Fraud”
Event & Risk Assessment “Think like a Fraudster”

Proactive Fraud Detection Cycle
Today

- 10th Anniversary Enron; 35th ISACA; ACFE 24th
- Impact of Data Analysis on Fraud Detection
- ISACA: “Data Analytics – A Practical Approach”
- Possible roles for audit in the fight against fraud
- What is a COSO based proactive fraud firewall
- Highlights of the fraud that started it all!

1. The ACFE breaks Occupational Fraud into 3 areas. What are they?
2. Which one is the most common? Costs the most?
3. About EDPAA/ISACA: (why relevant to ACFE?)
   - Why? – “Auditing through the computer not around”
   - Results: Most auditors indicate gathering the data is a challenge/barrier.
4. Is Data Analysis skills a core competency for a CFE?
5. Most organizations do not test their “fraud readiness” until after a fraud occurs.

Is Fraud a problem?

- Our company does not have a fraud problem.
- Our employees are honest & would not commit fraud.
- We only hire honest employees.
- Small frauds are not important to bother with.
- We follow all government regulations so we are protected against fraud.

Signs of Complacency

Executive gets prison for theft

The former chief financial officer must pay back nearly $1 million that she embezzled, a judge ruled.

By NEW YORK TIMES

Vicki, a former chief financial officer, pleaded guilty to embezzlement.

Results: The fraud ended with the bankruptcy of the company she embezzled.

- Why? – “Auditing through the computer not around”
- Results: Most auditors indicate gathering the data is a challenge/barrier.

Wake Up Call!
Insurance Manager Arrested on Fraud Charge

MIAMI — The administrative manager of an insurance company’s metropolitan New York office was arrested last weekend in Key West, Fla., on wire fraud charges, according to a Federal Bureau of Investigation spokesman here.

Paquale Ililo Agnese, 38 years old, allegedly stole about $12 million over the past three years from Pan American World Airways Inc.’s account with the insurance company, the FBI spokesman said.

According to the spokesman, Mr. Agnese credited Pan Am’s account with adjustments that weren’t due the airline company. He then diverted the false adjustments and spent the funds on cars and other personal items, the spokesman said.

Indisputable Video Evidence

If you know the scenario, it is just a matter of tracking down the evidence, right?

MY “WAKE-UP” Call $12.9 million

It Should be a CRIME to not know COSO

- THE CONTROL ENVIRONMENT - foundation for the IC system with discipline and structure.
- RISK ASSESSMENT - identification/analysis by management—not IA — risks relevant to achieve predetermined objectives.
- CONTROL ACTIVITIES - policies, procedures, and practices to be sure management objectives are achieved and risk mitigation strategies are carried out.
- INFORMATION AND COMMUNICATION - support all IC components by communicating IC responsibilities to employees and provides information that allows people to carry out their duties.
- MONITORING - oversight of IC by management or others outside the process; manual or automated; evidence objectives are met.
Role of Internal Auditing in Fraud

• What does your Charter say?

• Reference to GTAG 13 – Questions for CAE to ask senior management and Audit committee.

• Audit Committee Event Matrix.

• Each business system has a finite and predictable list of fraud schemes, typically five to seven.

• Each scheme permutation creates a finite and predictable list of fraud scenarios.

• The key to fraud location is to “proactively” look where fraud occurs.

• You need to know what fraud looks like particularly “in the data”.

• You do have to “LOOK”!

<table>
<thead>
<tr>
<th>Event</th>
<th>Magnitude</th>
<th>Improbability</th>
<th>Audit Merging</th>
<th>Annual Reporting</th>
<th>Annual Survey</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Deterioration, fraud, theft</td>
<td>$100,000</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 Major control breakdowns</td>
<td>More than $100,000</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 Involving collusion</td>
<td>More than $100,000</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4 Minor $10,000</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5 Involving minor management</td>
<td>All</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6 Denial of IT access to people or data</td>
<td>All</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7 Use ofEthics Policy</td>
<td>All</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8 Use management</td>
<td>All</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9 Misuse management</td>
<td>All</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10 Discussion of replacement of the CIO</td>
<td>All activity in advance</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Fraud is an Adaptive Crime

• Each business system has a finite and predictable list of fraud schemes, typically five to seven.

• Each scheme permutation creates a finite and predictable list of fraud scenarios.

• The key to fraud location is to “proactively” look where fraud occurs.

• You need to know what fraud looks like particularly “in the data”.

• You do have to “LOOK”!

Timing Is Everything!

Audit Path/Evolution of Data Analysis

<table>
<thead>
<tr>
<th>World Class</th>
<th>Continuous Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>Great</td>
<td>Centralized</td>
</tr>
<tr>
<td>Good</td>
<td>Repeatable</td>
</tr>
<tr>
<td>Average</td>
<td>Ad Hoc</td>
</tr>
</tbody>
</table>

ISACA White Paper
Impact of tools in the auditor’s hands

Read about fraud cases all the time. Auditors can ask good questions and listen to the answers. But what really sets them apart is they can Go Look and they have the ears of senior management and the board of directors.

Reality Check

- **Fraudsters** – Learn how to create the fraud and have the time and patience to get good at it. They start out slow, easy to explain and then increase the activity. Very creative at disguising fraud.

- **Auditors** – Need to learn what fraud looks like in the workplace. Per the PCAOB, auditors are often too predictable, polite, and easily sidetracked with heavy workloads.

Definitions

**Data analysis** tools are used to extract useful information from large volumes of data, with a key focus on improving efficiencies and effectiveness. Routine analysis may identify inconsistent, unusual or abnormal data instances.

**Data mining** is used to dive below the surface of these “flags” to see if a valid anomaly exists. By taking the extra step, the reviewer may uncover errors, waste or even outright fraud. Early detection of issues in the data improves the chances of recovery and prevents frauds from growing into disasters.

Example – Pivot Table
Step 1: Governance – *Tone at the Top*

1. External Audit of Financial Statements
2. Code of Conduct
3. Management Certification of Financial Statements
4. Manage Review/approvals/line of authority
5. Internal Auditing Function
6. External Audit of ICORF
7. Independent Audit Committee
8. Employee Support Programs
9. Fraud Training for Managers/executives
10. Fraud Investigation Policy
11. Hotline
12. Fraud Training for employees
13. Surprise Audits
14. Job rotation/mandatory vacation
15. Rewards for Whistleblowers
16. Key performance measuring/monitoring
17. Hiring – background and reference checks
18. Termination - exit interview process
19. Crime coverage - list of employees covered
20. Appoint A Chief of Company Anti-Fraud Policy

**Report to the Nations 2010**

Frequency of Anti-Fraud Controls by Size of Victim Organization

**Internal Control Environment**

<table>
<thead>
<tr>
<th>Control</th>
<th>Initial &amp; &amp;</th>
<th>Report</th>
<th>Defined &amp;</th>
<th>Measured</th>
<th>Automated</th>
<th>Optimized</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bal Revs</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Code of Conn</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Manage Revs</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Manage Revs</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Internal Auditing</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>External Audit</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Employee Support Programs</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Fraud Training</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Receivs</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Fraud Investigation Policy</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Med Revs</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>External Audit</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Employee Support Programs</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Fraud Training</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>External Audit</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Employee Support Programs</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Fraud Training</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>External Audit</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Auditing Tone at the Top

• Review Board Minutes
• Did management attend Code of Conduct Training
• Audit Expense Reports
• Hotline “reports” Follow-up
• Handling Code of Conduct “exceptions”
• Review Board of Directors duty training
• Did BoD conduct a self-assessment
• Benchmark against peer organizations

Step 2: Fraud Investigation

<table>
<thead>
<tr>
<th></th>
<th>How and when to start an investigation</th>
<th>How &amp; when to elevate the investigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Who can approve</td>
<td>Consistency &amp; uniformity, similar offenses treated alike</td>
</tr>
<tr>
<td>2</td>
<td>Documentation Requirements</td>
<td>Guidance - how far to pursue investigation</td>
</tr>
<tr>
<td>3</td>
<td>Data Analysis Needs</td>
<td>Communications - before, during &amp; after investigation</td>
</tr>
<tr>
<td>4</td>
<td>Designate the members of the team</td>
<td>Extent of recovery efforts to be conducted</td>
</tr>
<tr>
<td>5</td>
<td>Process for adding experts to the team</td>
<td>Issue final written report</td>
</tr>
<tr>
<td>6</td>
<td>Access, evaluate &amp; mitigate internal controls</td>
<td>Records retention</td>
</tr>
</tbody>
</table>

How To Audit

• Actually look at recent investigations and determine if the investigators followed the policy.
• Be alert for inconsistencies; low level full investigation; higher level nothing.
Adding experts skilled in data analysis can get the complete picture.

Why not use internal auditing staff?

Impact changes if the company has a Crime or fidelity insurance policy.

**Sequence of Fraud Activities**

Lessons Learned influence future use of prevention and control processes.

**Step 3: Fraud Risk Assessment**

**Think Like a Fraudster!**

- Is a fraud risk assessment the same thing as an anti-fraud review?
- Will a fraud brain storming session prior to each audit meet IIA 2120.A2 standard?
- Have you conducted an anti-fraud review?
- Can data analysis improve audit’s ability to detect fraud sooner?
**Classic Risk Analysis**

- Defining threats and vulnerabilities
- Assessing likelihoods and probabilities
- Evaluating scope and magnitude
- Consider Controls and counter measures
- Trace the scenarios to the appropriate database(s) and identify the key data requirements.

**Events & Risk Assessment**

**Think Like A Fraudster!**

Brainstorming and CSA for areas prone to fraud

Many templates exist – find one you like best. Brainstorming and CSA for areas prone to fraud

---

**Most Common Approach – The CSA**

- Understand where fraud is likely to occur.
- Reach across the organization to gather as many opinions about fraud occurrence.
- Recognize that participants will have difficulty in envisioning fraud happening.
- Use anonymous polling software to open discussions in sensitive areas.
- Consider everyone’s opinion (outlier concerns).

**Example “Brainstorming Session”**

Automated System:

1. Cashiers handle the same number of sales
2. Cashiers should receive about the same number of refunds or returns
3. Employees should not receive “refunds”
4. All invoices should be sequential without gaps
5. Refunds are computed amounts, therefore their distribution should follow Benford’s law
Example “Brainstorming Session”

5. An automated system should not allow duplicate refunds
6. Customer can not be refunded more than what they paid originally
7. Supervisor overrides should all be within business hours (not outside the normal day)
8. Correlation between sales and refunds as refunds follow the sales (trending)

Step 4: Controls Testing - Look for Fraud

- Just because you have completed the fraud risk assessment does not mean you are done.
- Many companies do not proactively test their fraud readiness until after a fraud occurs.
- By taking advantage of the rich knowledge embedded in the fraud risk assessment template, internal auditing can incorporate detail audit tests into their audit universe.
- As future audit schedules are developed, the more important risks to the organization should float to the top of the priority scale.

Testing Entity & Process Controls

<table>
<thead>
<tr>
<th>Anti-fraud Lessons Learned Embedded Into the IA Function</th>
<th>Control Embedded?</th>
<th>Control Quality Guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Functional Leadership</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Leading Practices &amp; Technology Tools</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. 100% Audit Universe - No Day Areas</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Risk Based Audit Engagement Planning</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Maintain Organizational &amp; Named Staff</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Either the PPP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Audit Results</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. Stakeholder Satisfaction</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Are fraud risk flags imbedded into audit programs? Is the staff fully trained in technology? If you do not look, then who will....

Embed Analytics Into Audit Programs

Sample data mining internal auditing program for payroll

1. **Stratify** paid amounts, hours worked, hourly rates and check dates for unusual trends and exceptions
2. **Reconcile** salaried employee gross pay from one pay period to the next
3. **Compare** payroll costs from one period to another
4. **List/extract** all hourly employees working more than the total hours available in the week
Sample data mining internal auditing program for payroll (continued)

5. Compare payroll data files to HR data files to detect additional/missing employees and differing salary rates
6. List possible duplicate payments based on the same day and employee
7. List possible duplicate payments based on the check date and the check amount absolute value
8. Review the sequence of check numbers for gaps

Step 5: Ongoing Monitoring

• The end.....

• Equity Funding Fraud
  – 2 years to investigate
  – First large scale use of the computer to commit financial statement fraud
  – 9 people served jail time including two auditors
  – 64,000 “fake” life insurance policies created
Now that internal controls are finally embedded in the critical business processes that drive enterprise success, the strategic spotlight has shifted. Where? To monitoring.

Monitoring = Compliance?

- COSO principles 19 & 20 - Monitoring procedures ....internal control system operates effectively over time & deficiencies identified and communicated in a timely manner to those parties responsible for taking corrective action

- USA Sentencing guidelines – periodic reviews of a company’s compliance program, using internal resources, such as a company’s internal audit

- OECD Good Practice - risks should be regularly monitored to ensure continued effectiveness of the company’s IC’s, ethics, and compliance program.

- UK Bribery Act - ongoing risk review and monitoring and a compliance program should be reviewed regularly and encourages higher risk and larger companies to consider external verification or assurance of the effectiveness of anti-bribery policies.

Questions?

Don Sparks, CISA, CIA, ARM
dons@audimation.com

Founded in 1992, Audimation Services, Inc. is a leader in providing data analysis technology to help companies understand their data, assess risks, test controls, and fight fraud.

As the sole U.S. distributor of IDEA, CaseWare™ Monitor and SmartExporter for SAP, we help our clients maximize their technology investments by providing support, training and other valuable resources.