Using analytics to your advantage – interpretations from COSO’s new Fraud Risk Program Guidance
Topics for discussion

About the new COSO Fraud Risk Guidance to Principle #8
Mapping COSO to fraud risks and analytics examples
Fraud risk governance
Analytics use case examples
About the new COSO Fraud Risk Guidance to Principle #8
Progressing with the times
About the new COSO Guidance

- Stems from 2013 Internal Controls Framework
- Specifically addresses Principle #8 – Fraud Risk Assessment
- Incorporates previous ACFE / IIA / AICPA publication on “Managing the Business Risk of Fraud”
- Released September 2016
- Maps to the 17 COSO Internal Controls Principles set forth in the 2013 Framework
- Increased focus on data analytics
- Scope is broader than just doing “fraud risk assessments”
More than just a fraud risk assessment

Guide includes guidance on establishing an overall fraud risk management program including:

► Establishing fraud risk governance policies
► Performing a fraud risk assessment
► Designing and deploying fraud prevention and detect control activities
► Conducting investigations
► Monitoring activities
### ROI considerations

2016 ACFE Report to the Nations

Companies without data monitoring/analytics in place suffered a median loss per incident of **$200k** vs. **$92k** with data analytics in place.

20 investigations per year x $102k = $2.16M in savings per year.

#### Figure 59: Median Loss Based on Presence of Anti-Fraud Controls

<table>
<thead>
<tr>
<th>Control</th>
<th>Percent of Cases</th>
<th>Control in Place</th>
<th>Control Not in Place</th>
<th>Percent Reduction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proactive Data Monitoring/Analysis</td>
<td>36.7%</td>
<td>$92,000</td>
<td>$200,000</td>
<td>54.0%</td>
</tr>
<tr>
<td>Management Review</td>
<td>64.7%</td>
<td>$100,000</td>
<td>$200,000</td>
<td>50.0%</td>
</tr>
<tr>
<td>Hotline</td>
<td>60.1%</td>
<td>$100,000</td>
<td>$200,000</td>
<td>50.0%</td>
</tr>
<tr>
<td>Management Certification of Financial Statements</td>
<td>71.9%</td>
<td>$104,000</td>
<td>$205,000</td>
<td>49.3%</td>
</tr>
<tr>
<td>Surprise Audits</td>
<td>37.8%</td>
<td>$100,000</td>
<td>$195,000</td>
<td>48.7%</td>
</tr>
<tr>
<td>Dedicated Fraud Department, Function, or Team</td>
<td>41.2%</td>
<td>$100,000</td>
<td>$192,000</td>
<td>47.9%</td>
</tr>
<tr>
<td>Job Rotation/Mandatory Vacation</td>
<td>19.4%</td>
<td>$99,000</td>
<td>$170,000</td>
<td>47.6%</td>
</tr>
<tr>
<td>External Audit of Internal Controls over Financial Reporting</td>
<td>67.6%</td>
<td>$105,000</td>
<td>$200,000</td>
<td>47.5%</td>
</tr>
<tr>
<td>Fraud Training for Managers/Executives</td>
<td>51.3%</td>
<td>$100,000</td>
<td>$190,000</td>
<td>47.4%</td>
</tr>
<tr>
<td>Fraud Training for Employees</td>
<td>51.6%</td>
<td>$100,000</td>
<td>$188,000</td>
<td>46.8%</td>
</tr>
<tr>
<td>Formal Fraud Risk Assessments</td>
<td>39.3%</td>
<td>$100,000</td>
<td>$187,000</td>
<td>46.5%</td>
</tr>
<tr>
<td>Employee Support Programs</td>
<td>56.1%</td>
<td>$100,000</td>
<td>$183,000</td>
<td>45.4%</td>
</tr>
<tr>
<td>Anti-Fraud Policy</td>
<td>49.6%</td>
<td>$100,000</td>
<td>$175,000</td>
<td>42.9%</td>
</tr>
<tr>
<td>Internal Audit Department</td>
<td>73.7%</td>
<td>$123,000</td>
<td>$215,000</td>
<td>42.8%</td>
</tr>
<tr>
<td>Code of Conduct</td>
<td>81.1%</td>
<td>$120,000</td>
<td>$200,000</td>
<td>40.0%</td>
</tr>
<tr>
<td>Rewards for Whistleblowers</td>
<td>12.1%</td>
<td>$100,000</td>
<td>$163,000</td>
<td>36.7%</td>
</tr>
<tr>
<td>Independent Audit Committee</td>
<td>62.5%</td>
<td>$114,000</td>
<td>$180,000</td>
<td>36.7%</td>
</tr>
<tr>
<td>External Audit of Financial Statements</td>
<td>81.7%</td>
<td>$150,000</td>
<td>$175,000</td>
<td>14.3%</td>
</tr>
</tbody>
</table>
Mapping the COSO Framework to fraud risks
An integrated platform for anti-fraud monitoring and response

Visualization: Detect fraud risks within a business process, taking a risk-based approach

Case Management: Assign tasks, flag transactions and delegate projects for review

Statistical: Apply predictive modeling and anomaly detection to surface hidden risks or new patterns

Pattern & Link: Uncover hidden relationship or conflicts of interest

Detect

Investigate

Respond

Discover
COSO 2013 Internal Controls Framework
Principles 1 through 5

1. The organization demonstrates a commitment to integrity and ethical values.

2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

1. The organization establishes and communicates a fraud risk management program that demonstrates the expectations of the board of directors and senior management and their commitment to high integrity and ethical values regarding managing fraud risk.

- Executive reporting
- Interactive dashboards
- Targeted analysis around metrics, compliance and ratios
COSO Framework
Principles 6 through 9

6. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

7. The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.

8. The organization considers the potential for fraud in assessing risks to the achievement of objectives.

9. The organization identifies and assesses changes that could significantly impact the system of internal control.

2. The organization performs comprehensive fraud risk assessments to identify specific fraud schemes and risks, assess their likelihood and significance, evaluate existing fraud control activities, and implement actions to mitigate residual fraud risks.

Analytic Considerations

- Surveys & heat maps
- Media scans and external sources such as industry news
- Complaints database
COSO Framework
Principles 10 through 12

10. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

11. The organization selects and develops general control activities over technology to support the achievement of objectives.

12. The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.

3. The organization selects, develops, and deploys preventive and detective fraud control activities to mitigate the risk of fraud events occurring or not being detected in a timely manner.

- ABaC analytics
- P2P, O2C, T&E, CRM analysis
- General ledger transaction analysis

COSO Framework Principles 13 through 15

13. The organization obtains or generates and uses relevant, quality information to support the functioning of other components of internal control.

14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

15. The organization communicates with external parties regarding matters affecting the functioning of other components of internal control.

4. The organization establishes a communication process to obtain information about potential fraud and deploys a coordinated approach to investigation and corrective action to address fraud appropriately and in a timely manner.

- Case management
- Escalation and triage
- Review workflow management
COSO Framework
Principles 16 & 17

16. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

17. The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors.

5. The organization selects, develops, and performs ongoing evaluations to ascertain whether each of the five principles of fraud risk management is present and functioning and communicates fraud risk management program deficiencies in a timely manner to parties responsible for taking corrective action, including senior management and the board of directors.

- Investigative procedures
- Deep dive analysis
- Email and communications review

Monitoring Activities

COSO Framework Principles

Fraud Risk Management Principles

Analytic Considerations

5. The organization selects, develops, and performs ongoing evaluations to ascertain whether each of the five principles of fraud risk management is present and functioning and communicates fraud risk management program deficiencies in a timely manner to parties responsible for taking corrective action, including senior management and the board of directors.

- Investigative procedures
- Deep dive analysis
- Email and communications review

Investigative procedures
Deep dive analysis
Email and communications review

Analytic Considerations
Graphic 1: Forensic Data Analytics Process used in COSO guidance

<table>
<thead>
<tr>
<th>Analytics Design</th>
<th>Data Collection</th>
<th>Data Organization &amp; Calculations</th>
<th>Data Analysis</th>
<th>Findings, Observations &amp; Remediation</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Identify risks based on industry &amp; company-specific knowledge</td>
<td>• Work with information technology personnel to map identified tests to relevant data sources</td>
<td>• Execute on the analytics work plan</td>
<td>• Evaluate initial analytics results</td>
<td>• Request supporting documents and/or validate as available</td>
</tr>
<tr>
<td>• Map risks to appropriate data sources and assess availability</td>
<td>• Assess data integrity and completeness</td>
<td>• Modify analytics as appropriate based on data received, data quality and user feedback</td>
<td>• If possible, develop scoring model and prioritize transactions or entities based on multiple risk attributes</td>
<td>• Determine sample selections, or triage/escalation procedures</td>
</tr>
<tr>
<td>• Develop work plan and define analytics and procedures</td>
<td>• Extract, transform / normalize and load data into the analytics platform</td>
<td>• Consider integrating advanced analytics procedures such as text mining, statistical analysis and pattern / link analysis</td>
<td>• Tune the model as needed to refine results for relevancy</td>
<td>• Develop remediation and/or investigative plan</td>
</tr>
<tr>
<td>• Define engagement timeline and deliverables</td>
<td>• Validate that data has been loaded completely and accurately</td>
<td></td>
<td></td>
<td>• Escalate findings as appropriate and track dispositions</td>
</tr>
</tbody>
</table>
Fraud risk governance
Who owns fraud?
Having a seat at the table from a governance perspective

Companies are creating plans to address fraud proactively and reactively

- Setting the proper tone
  - Code of ethics/tone at the top
  - Fraud prevention policies
- Communication and training
  - Fraud risk assessment
- Controls monitoring
- Fraud response plan
- Improving
  - Assess
  - Proactive
  - Reactive
- Monitor
  - Communicate
  - Proactive and reactive response to fraud

- Executive mgmt
- Audit committee
- Controllers group
- Internal audit
- IT
- HR
- General counsel
- Compliance
- Security
Why people commit fraud: the fraud triangle
Cressey’s “fraud triangle”

Companies are decentralized, with inconsistent internal controls

Lack of infrastructure and controls in locations

Layoffs and salary cuts create personal financial hardship

Tight credit environment

Stock prices are unstable

More regulatory focus increased

Budgets are decreasing; companies and organizations are doing more with less

Companies are downsizing, impacting internal controls

Large projects and acquisitions increase risks of costs not being noticed

Stressed and disgruntled employees may have greater ability to rationalize improper actions

Dissatisfaction with compensation compared to peers and supervisors

Opportunity

Opportunity to commit fraud

Pressure

Rationalization
Fraud tree: Need to consider all three categories

New website coming:

Fraud Tree

- Corruption
  - Conflicts of Interest
  - Bribery/Corruption/FCPA
  - Illegal Gratuities
  - Bid-Rigging/Procurement

- Fraudulent Statements
  - Revenue Recognition
  - Reserves
  - Non Financial

Asset Misappropriation

- Cash Larceny
- Theft of Other Assets – Inventory/AR/Fixed Assets
- Fake Vendor
- Payroll Fraud
- T&E Fraud
- Theft of Data (incl. cyber)

Traditional focus of compliance and legal

Traditional focus of external auditors

Traditional focus of internal auditors and SOX compliance
Frequent compliance analytics risk areas, particularly in emerging markets

<table>
<thead>
<tr>
<th>Meals &amp; Entertainment</th>
<th>Marketing &amp; Events</th>
<th>CRM and Sales</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Security/Insider Threat</td>
<td>Employee Payroll</td>
<td>Sales, Distributor &amp; Margin Analysis</td>
</tr>
<tr>
<td>Vendor Payments / AP</td>
<td>Capital Projects</td>
<td>Accounting Reserves</td>
</tr>
<tr>
<td>Inventory</td>
<td>3rd Party Due Diligence &amp; Watchlist, Shell Companies</td>
<td>Charity &amp; Donations</td>
</tr>
</tbody>
</table>

**Emerging monitoring activities may include...**

| Social Media Monitoring | Advanced Email Monitoring | Mobil Devices |
Analytics use cases
Big data techniques to counter fraud

- Multiple data sources – structured and unstructured
- Data visualization
- Text analytics
- Payment/transaction risk scoring
- Predictive modeling – technology assisted monitoring
- Case management, issue coding and built in workflow
- Flexible deployment models
Dashboard examples

Plan and build tests for:
- Payment risk scoring
- Vendor risk scoring
- High risk transactions
- Revenue recognition or sales commissions
- Conflicts of interests

Additional tests for enhanced reviews:
- Inventory management
- Salaries & payroll
- Employee travel & entertainment
- FCPA/UKBA (corruption risks)
- Selected compliance topics

Interactive dashboards in the hands of the business users
Risk ranking

Find high risk and most exposed third party vendors

Look at the details for each vendor to understand what tests are being triggered.
Data visualization: Accounts payable monitoring

High risk payment descriptions
Forensic data analytics framework
An integrated, platform – from a work flow and monitoring perspective

Audit, Shared Services, Compliance

Investigative mindset

Repeat the process: Continuous Auditing

Triage, Stop Payment and/or Sample Audit Selection

Big data processing platform

Monitoring & Detection Tools

Investigation Tools

Library of Counter Fraud tests

Text mining & advanced search

Visualisation & Risk Ranking

FINANCIAL ACCOUNTING DATA

MASTER & REFERENCE DATA

INTERNAL RISK ELEMENTS

EXTERNAL, SOCIAL MEDIA DATA

structured

unstructured

CASE MANAGER, TASK DELEGATION AND DATA REFRESH / SCRIPTING AUTOMATION

Watson / Cognitive

Statistical & Predictive

Pattern Matching

Case Manager, Task Delegation and Data Refresh / Scripting Automation

Investigation Tools

Statistical & Predictive

Watson / Cognitive

Pattern Matching

Case Manager, Task Delegation and Data Refresh / Scripting Automation

Investigation Tools

Statistical & Predictive

Watson / Cognitive

Pattern Matching

Case Manager, Task Delegation and Data Refresh / Scripting Automation

Libraries of Counter Fraud tests

Text mining & advanced search

Visualisation & Risk Ranking

FINANCIAL ACCOUNTING DATA

MASTER & REFERENCE DATA

INTERNAL RISK ELEMENTS

EXTERNAL, SOCIAL MEDIA DATA

structured

unstructured

CASE MANAGER, TASK DELEGATION AND DATA REFRESH / SCRIPTING AUTOMATION

Watson / Cognitive

Statistical & Predictive

Pattern Matching
Current challenge - Legacy surveillance & anti-fraud tools are falling short

► Legacy surveillance technologies suffer from overreliance on rule-based triggers, ranging from simple if-then statements to basic “keyword” searches on text fields and electronic communications…both of which can be easily circumvented.

► The approach described above results in increasing volumes of surveillance alerts and false positives, while real threats get buried and go undetected.

► A tool, in and of itself, will never be effective without the support by the right team with the right skills sets.
Five success factors in deploying forensic data analytics

1. Focus on the low hanging fruit, the priority of the first project matters
2. Go beyond traditional “rules-based” tests – incorporate big data thinking
3. Communicate: share information on early successes across departments / business units to gain broad support
4. Leadership gets it funded, but interpretation of the results by experienced or trained professionals make the program successful
5. Enterprise-wide deployment takes time, don’t expect overnight adoption
Thank you

Vincent Walden
Partner, EY Fraud Investigation & Dispute Services
404-817-5717
vincent.walden@ey.com
About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

Ernst & Young LLP, an equal opportunity employer, values the diversity of our work force and the knowledge of our people.

© 2016 Ernst & Young LLP. All Rights Reserved.

SCORE no. XX0000

1603-1886034
ED none

EY is committed to reducing its impact on the environment. This document was printed using recycled paper and vegetable-based ink.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com